Dissertation
On

ROLE OF JUDICIARY IN PROTECTING VICTIMS OF CYBER CRIME AGAINST WOMEN IN INDIA

LL.M. Dissertation submitted in the partial fulfillment of the requirements for the Degree of Master of Laws at the Sister Nivedita University (SNU)

Kolkata

Submitted By:

SHAMREEN NAAZ

Enrollment Number: 2322215005023

Registration Number : 230050239313

Session : 2023-2025

Under the Guidance of:

PROF: SOMANJANA DUTTA CHATTAKHANDI

(Assistant Professor, School of Law)

Sister Nivedita University

Department of Law

Sister Nivedita University

202

Sister Nivedita University
DG Block, ½ (New Town), Action Area 1, Kolkata- 7000156.
Phone: +91-7595044470, 75950444709, 830653112
Official Website: https://snuniv.ac.in
Email: info@snuniv.ac.in

Certificate

This is to certify that the Dissertation titled **"Role of Judiciary in Protecting Victims of Cyber Crime Against Women in India"** has been submitted by **Shamreen Naaz**, bearing Enrollment ID No.: 2322215005023, Registration No.: 230050239313, for partial fulfilments of the Degree of Master of Laws (LL.M) from Sister Nivedita University under my guidance. It is her original work and may be placed before the examiners for evaluation.

This research work has not been submitted for the award of any other degree of this University or of any other University.

Date: 25.04.25

Place: Kolkata.

Somanjana Dutta Chattakhandi

Assistant Professor, School of Law (SNU)

DECLARATION BY THE STUDENT

I hereby declare that the work which is being presented in this dissertation entitled "Role of Judiciary in Protecting Victims of Cyber Crime against Women in India" in partial fulfilment of the requirements for the award of the degree of Masters of Law in Criminal Law is an authentic record of my own work carried out during the period from 2023 to 2025 under the supervision of Somanjana Dutta Chattakhandi, Department of Law, SNU Kolkata.

I acknowledge that I have read and understood the UGC regulations, 2018 (*Promotion of Academic integrity and Prevention of Plagiarism in Higher Educational Institutions*).

I confirm that this dissertation has been checked for plagiarism using the plagiarism checking software Turnitin. At the end of the dissertation, a copy of the summary report demonstrating similarities in content and its potential source (if any), generated online using plagiarism checking software is enclosed. I herewith confirm that the dissertation has been less than 10% similarity according to the plagiarism checking software's report and meets the UGC Regulations as well as plagiarism rules of Sister Nivedita University.

I further declare that no portion of the dissertation or its data will be published without the Institute's or supervisor's permission. I have not previously applied for any other degree or award using the topics and findings described in my dissertations.

Shamreen Naaz

Name of the Student : **SHAMRREN NAAZ**

Registration no- : **230050239313**

Department : **Law**

PREFACE

In an era dominated by digital transformation, the lives of individuals have been significantly influenced by technology—bringing convenience, but also giving rise to novel threats. Among the most alarming of these is cybercrime, which disproportionately affects women by invading their privacy, dignity, and mental well-being. While cyberspace offers opportunities for communication and empowerment, it has also become a domain where harassment, stalking, defamation, and abuse of women occur with increasing frequency and severity

This dissertation, titled "Role of Judiciary in Victim Protection in Cases of Cyber Crime Against Women in India", seeks to critically examine the judicial landscape that governs the protection of women from such online offences. The research aims to evaluate the adequacy of existing legal provisions, the responsiveness of the Indian judiciary, and the effectiveness of victim-centric remedies.

The motivation behind this study stems from the rising statistics of cyber offences against women in India and the evident challenges in law enforcement and judicial redressal. While laws such as the Information Technology Act, 2000, and relevant sections of the Indian Penal Code provide a foundational framework, the real test lies in their interpretation and application by the judiciary.

Throughout the course of this research, I have attempted to assess how Indian courts have contributed to shaping victim-sensitive jurisprudence, the role of judicial activism, and the gaps that persist in the practical execution of protective measures. Comparative insights from global jurisdictions have also been explored to identify best practices that can inform judicial reform in India.

This work would not have been possible without the guidance of my mentors, the support of my peers, and the strength drawn from the stories of countless women who continue to courageously navigate the challenges of digital abuse. It is my hope that this study contributes meaningfully to the discourse on gender justice
in the digital age and encourages a more robust and empathetic judicial response to cybercrime against women.

ACKNOWLEDGEMENT

I am deeply indebted to Prof. Somanjana Dutta Chattakhandi, School of Law, Sister Nivedita University, New Town, Kolkata, who amidst her many engagements found time to guide me with unflagging interest and bestowed me invaluable suggestion and constant encouragement throughout the period of my research work.

I am grateful to Prof. (Dr.) Debashree Mukherjee and the entire faculty members of Sister Nivedita University, New town, Kolkata for having constantly helped and have been generous in providing me the necessary time and valuable suggestions to complete the work.

I record my deep sense of feelings and gratitude to my parents, brother and also my friends for constant inspiration and support.

I am also eternally grateful to my God and savior for giving me the intellect, motivation, passion and ability to strive for better things.

At last my sincere thanks to all those helped me in completing the thesis work mentioned above.

Place : Kolkata

Date. : 25.04.25

Shamreen Naaz

Shamreen Naaz

List of Abbreviation

AI	Artificial Intelligence
AIR	All India Reporter
BNS	Bharatiya Nyaya Sanhita, 2023
BNSS	Bharatiya Nagarik Suraksha Sanhita, 2023
BSA	Bharatiya Sakshya Adhiniyam, 2023
CPR.	Centre for Policy Research
CCTV	Closed-Circuit Television
FIR	First Information Report
ICT	Information and Communication Technology
IPC	Indian Penal Code, 1860
IT Act	Information Technology Act, 2000
ITAA	Information Technology (Amendment) Act, 2008
NCRB	National Crime Records Bureau
NCW	National Commission for Women
NGO	Non – Governmental Organisations
NCPR	National Commission for Protection of Child Rights
OUP	Oxford University Press
POCSO	Protection of Children from Sexual Offences Act, 2012
SC	Supreme Court
SCC	Supreme Court Cases
SCW	State Commission for Women
UK	United Kingdom
UNCITRAL	United Nations Commission on International Trade Law
US / USA	United States of America
WWW	World Wide Web

List of Cases

1. Ritu Kohli v. Manish Kathuria, 2001 Cri LJ 2801 (Delhi)
2. Sukanta Halder v. State of West Bengal, AIR 1952 Cal 214
3. State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004.
4. Justice K.S. Puttaswamy (Retd.) & Anr. V. Union of India & Ors., (2017) 10 SCC 1
5. Shreya Singhal v. Union of India is (2015) 5 SCC 1; AIR 2015 SC 1523
6. Kharak Singh vs State of UP AIR 1963 SC 1295 and M.P Sharma vs Satish Chandra, AIR 1954 SC 300
7. Kalandi Charan Lenka v. State of Odisha 2017 SCC OnLine Ori 52
8. Anil Kumar Srivastava v. Additional Director, Medical Health and Family Welfare 2005 (3) ESC 1917
9. Karmanya Singh Sareen & Anr. V. Union of India & Ors., (2016) 233 DLT 436 (Delhi HC)
10. Ranjit D. Udeshi v. State of Maharashtra, (1965) AIR 881, 1965 SCR (1) 65
11. State of Maharashtra (1965) and Aveek Sarkar v. State of West Bengal, (2014) 4, SCC 257
12. Sampurna Behura v. Union of India (2018) 4 SCC 433
13. Mrs. X v. Union of India & Ors., 2023 SCC OnLine SC 818.
14. Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1.
15. State of Kerala v. Rahul Pasupalan & Anr., Crime No. 1820/2015, Cyber Cell, CBCID, (2019).
16. Sabu Mathew George v. Union of India (2018) 3 SCC 229
17. Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801
18. Prajwala v. Union of India, Writ Petition (Criminal) No. 194 of 2015
19. Ajay Goswami v. Union of India, (2007) 1 SCC 143
20. Yogesh Prabhu v. State of Maharashtra, (2015) Cri. Bail Appl. No. 2733 of 2015 (Bombay High Court)
21. Shamsher Singh Verma v. State of Haryana, (2016) 15 SCC 485
22. State v. Jayanta Das, Cr. Appeal No. 21 of 2017 (D&S Court, Khurda, Odisha)
23. Raghuraj Singh v. Air Force Bal Bharti School, CIC/LS/A/2011/000401, decided on 3 October 2011
24. State of Maharashtra v. Awadhesh Kumar Parasnath Pathak, 2024 SCC OnLine Bom 660
25. Prakhar Sharma v. State of Madhya Pradesh, 2018 SCC OnLine MP 934
26. Archana Sharma v. State of NCT of Delhi & Ors., W.P. (CRL) 1084/2020, Delhi High Court
27. Nipun Saxena Vs. Union of India, 2018, 10 SCC 703.

28. Nikhil Soni v. Union of India & Ors., D.B. Civil Writ Petition No. 7414/2006, decided on 10 August 2015 by the Rajasthan High Court.

29. Suresh v. State of Maharashtra, Criminal Writ Petition No. 1493 of 2018, decided on 31 July 2019 by the Bombay High Court (Aurangabad Bench).

Table of Contents

PARTICULARS	Page no.
CERTIFICATE	
SELFDECLARATION	
ACKNOWLEDGMENT	
LIST OF ABBREVIATION	
LIST OF CASES	
CHAPTER–1	**1 – 11**
1. **INTRODUCTION**	
1.1: Introduction	1 – 2
1.2 : Overview of Cyber Crime against Women	2 – 3
1.3 : Statement of Problem	3 – 4
1.4 : Literature Review	4 – 10
1.5:Research Objectives	10
1.6:Research Questions	10
1.7:Research Methodology	11
1.8:Hypothesis	11
1.9: Significance of the Study	11
CHAPTER – 2	**12 - 26**
2. CYBER CRIME TARGETTING WOMEN: CHARACTERISTICS AND ISSUES	
2.1: Understanding Cyber Crime	12 – 13
2.2:Growth of Cyber Crime in India	13 – 14
2.3: Types of Cyber Crime against Women	14
2.3.2: Cyber harassment	16 – 17
2.3.3: Cyber Pornography	17 – 18
2.3.4: Cyberbullying and Trolling	18 – 19
2.3.5: Non – Consensual Dissemination of Private Content	19 – 20
2.3.6: Phishing and Financial Fraud	20

Table of Contents

2.4: Advancement of Technology in Facilitating Cyber Offences	21 – 23
2.5: Role of Artificial Intelligence	24 – 26
CHAPTER – 3 LEGISLATIVE MEASURES CONCERNING CYBER CRIME TARGETTING WOMEN	**27 – 53**
3.1: Introduction	27 – 28
3.2: Constitutional Provisions	29 – 32
3.3: Bharatiya Sakshya Adhiniyam	32 – 34
3.3.1: Role of BSA in Combating Cyber Crime	34 – 36
3.4: Indian Penal Code	37 – 38
3.5: Bhartiya Nyaya Sanhita	39 – 41
3.6: BhartiyaNagarik Suraksha Sanhita	41 – 43
3.7: Information Technology Act, 2000 and It's Amendment	44 – 47
3.8: Other Legislation Safeguarding Women in the Digital Realm	**47 – 53**
3.8.1: Digital Personal Data Protection Act, 2023	47 – 50
3.8.2: Indecent Representation of Women (Prohibition) Act, 1986	51 – 53
3.9: Summary	53
CHAPTER – 4	**54 – 102**
4. **ROLE OF JUDICIARY IN PROTECTING VICTIMS OF CYBER CRIME AGAINST WOMEN**	
4.1: Introduction	54
4.2: Mrs. X v. Union of India and Others (2023)	55 – 58
4.3: Ritesh Sinha v. State of Uttar Pradesh (2019)	58 – 61
4.4: State of Kerala v. Rahul Pasupalan and Another (2019)	61 – 63
4.5: Sabu Mathew George v. Union of India (2018) 3 SCC 229	63 – 65
4.6: Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801	66 – 68
4.7: Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1	68 - 70
4.8: Shreya Singhal v. Union of India (2015) 5 SCC 1	71 – 73

Table of Contents

4.9: The Prajwala v. Union of India (2015)	73 – 76
4.10: Ajay Goswami v. Union of India (2007)	76 – 77
4.11: Yogesh Prabhu v. State of Maharashtra (2015)	78 – 81
4.12: State of Tamil Nadu v. SuhasKatti (2004)	81 – 84
4.13: Shamsher Singh Verma Vs State of Haryana (2016)	84 – 86
4.14: State v. Jayanta Das (2017) (Odisha)	86 – 89
4.15: Manish Kathuria Vs RituKohli (2001)	89 – 91
4.16: Raghuraj Singh v maw Air force Bal Bharti School, (2011)	91 – 93
4.17: State of Maharashtra v. Awadhesh Kumar Parasnath Pathak (2024)	93 – 95
4.18: Prakhar Sharma v. State of Madhya Pradesh (2018)	96 – 98
4.19: Archana Sharma vs State of NCT Of Delhi &Ors. Aka Bois Locker Room (2020)	99 – 102
4.20: Summary	102
CHAPTER – 5	**103 – 124**
5. **CHALLENGES IN VICTIM PROTECTION AND SUPPORT MECHANISMS**	
5.1. Psychological and Social impact on Victims	**103 – 105**
5.1.1: Psychological Factors	103 – 104
5.1.2: Sociological Reasons	104 – 105
5.2: Challenges in Access to Justice and Legal Remedies	**105 – 110**
5.2.1: Absence of Specific Legislation Addressing Cyber Crime	105 – 106
5.2.2: Challenges Encountered by Law Enforcement and the Judicial System in dealing Cybercrime Against Women.	106 – 107
5.3: Victim Blaming and Social Stigmatization	110 – 115
5.4: Evaluation of Existing Mechanisms for Victim Support and Their Effectiveness	115 – 118
5.5: Gaps and Effectiveness	118 – 121
5.6: The Information Technology (Intermediary Guidelines and Digital Media Ethic	121 – 123

Table of Contents

Code) Rules, 2021	
5.7 Summary	123 – 124
CHAPTER – 6	**125 – 138**
6. **COMPARATIVE LEGAL STUDY AND BEST PRACTICES**	
6.1 Global Efforts Against Cyber Crime:	125 – 129
6.2: The Budapest Convention	129 – 132
6.3: United States of America	133 – 134
6.4: United Kingdom	134 – 135
6.5: Australia	135 – 136
6.6: Effective Strategies for Preventing Cyber Crime Against Women	136 – 138
CHAPTER – 7	**139 – 146**
7. **CONCLUSION AND RECOMMENDATIONS**	
7.1: Conclusion	139 – 140
7.2: Recommendation	140 – 141
7.3: Government Initiatives and Policies	142 – 146
Bibliography	**147 – 149**

Chapter – 1

Introduction

1.1 : Introduction

In ancient India, women held an important position and were even celebrated in texts like the Vedas as creators. However, in today's world, women often encounter unfair treatment and inequality. There are instances where women are perceived as less significant than men, resulting in a substantial disparity between the genders. This biased perspective leads some men to believe that they can act without fear of repercussions. Cybercrimes exhibit similar patterns, as offenders in the digital realm frequently think they can evade justice.

Cybercrime poses a global concern that impacts everyone. As technology evolves, it jeopardizes individuals' privacy and security. In countries such as India, where technology is prevalent but awareness of legal rights is limited, this issue becomes even more apparent. The online landscape lacks physical boundaries, facilitating the ability of criminals to conceal their identities or impersonate others. [1]

A major concern Is that individuals with malicious intent often target women in online environments. Although India has established laws to combat cybercrime, these regulations do not adequately address the unique challenges encountered by women. Authorities, including the police, are not fully equipped to effectively respond to Cyber Crimes, especially those directed at women. The digital realm has turned into a breeding ground for crimes against women, consistently threatening their safety and privacy. In this virtual space, women frequently deal with issues like stalking, voyeurism, body shaming, defamation, and unwanted surveillance. Unlike physical violence, these cybercrimes tend to have a more significant impact on women's mental health. [2] While existing laws mainly focus on ensuring physical safety, mental health is just as vital. For context, approximately 850,000 adults in the United States, predominantly women, fall victim to cyber-stalking each year, and 40% of women have experienced violence while dating online.[3]

---

[1] B. Roy, Women's empowerment in India, from ancient period to modern time period, Times of India, Jan. 16, 2020,https://timesofindia.indiatimes.com/readersblog/scatteredthoughts/womens-empowerment-in-indiafrom-ancient-period-tomodern-time-period-46689

[2] P. Kaushik, Cyber Laws to Curb Cyber Victimization of Women in India and other developing Countries: A Comparative Critical Legal Analysis, 9th International Conference on Information Law and Ethics, Jan. 1, 2020.

[3] Each year, about 850,000 adults in the U.S., most of them women, are victims of cyberstalking. Additionally, 40% of women have reported facing violence in the context of online dating. (Sources: Cyber Civil Rights Initiative; Pew Research Center, Online Dating C Relationships, 2020)

In India, the situation concerning Cyber Crimes is quite severe, but the official statistics from the NCRB (National Crimes Record Bureau) may not fully capture the reality. The instances of Cyber Crime reported under the Information Technology Act surged by an astonishing 300% from 2011 to 2014. As per the NCRB, 21,796 Cyber Crime cases were documented in just 2017. This study seeks to analyze these figures and reveal the genuine obstacles India faces in addressing Cyber Crimes. The official crime data in India indicates that there are notable gaps in the existing laws pertaining to Cyber Crimes against women.[4]

In recent years, cyberspace has become an essential component of our everyday lives. With the growing use of technology, Cyber crime has emerged as a significant societal threat. Cybercrime encompasses a wide array of illegal activities conducted via the internet or any digital platform. It includes various offenses ranging from financial fraud, cyberbullying, and hacking to online harassment. Regrettably, women have been disproportionately impacted by cybercrime in India, where incidents of cyber offenses against them have rapidly escalated in recent years.

1.2 : Overview of Cyber Crimes Against Women

The rise of cyber crimes against women in India poses a significant challenge, impacting their mental health, physical wellbeing, and financial stability. The range of cyber crimes targeting women includes online harassment, cyber stalking, cyberbullying, revenge porn, and financial fraud. Online harassment stands out as one of the most prevalent forms of cybercrime against women in India and involves using digital channels to deliver threatening, abusive, or offensive messages or comments. A report from the National Commission For Women indicates that 54.8% of women have encountered cyber harassment. This type of harassment can lead to considerable mental distress, anxiety, and fear in women, making them feel insecure and vulnerable.[5]

Cyber stalking represents another form of cybercrime imposed on women in India. This refers to the recurring online harassment comprising following, monitoring, or tracking an individual's online activities. Cyber stalkers leverage various digital platforms, including social media, emails, and messaging applications, to pursue and torment their victims. According to a report from the

[4] NCRB data shows a 300% rise in cyber crime cases under the IT Act from 2011 to 2014, with 21,796 cases reported in 2017. However, actual figures may be higher due to underreporting. See: Crime in India 2017, NCRB, Ministry of Home Affairs.

[5] National Commission for Women, Cyber Crime Data Analysis, available at: https://ncw.nic.in [Accessed on 20th March 2025].

Cyber Crime Cell of Mumbai Police, there has been a 91% rise in cyber stalking incidents in India over the past year.[6]

Cyberbullying refers to the use of digital technology to harass, embarrass, or intimidate individuals. It is one of the prevalent forms of cybercrime targeting women, especially among young girls and women. Various forms of cyberbullying exist, such as disseminating rumors, posting insulting messages, and sharing compromising pictures or videos. A study conducted by the Cyber and Media Cell of the Delhi Police discovered that 40% of those affected by cyberbullying in India were women. [7]

1.3 : Statement of Problem

The swift expansion of digital technologies in India has resulted in a marked increase in cyber crimes aimed at women, creating considerable difficulties for law enforcement and victim protection systems. According to the National Crime Records Bureau (NCRB) report (2023), there has been a significant rise in cyber crimes targeting women, including incidents of cyberstalking, online harassment, and the unauthorized distribution of intimate images. For example, in 2022, Odisha recorded the highest number of cybercrime cases against women, totalling 542 incidents, underscoring the widespread nature of this issue across different states. [8]

Despite the existence of legislative measures and policy efforts intended to reduce such crimes, the efficacy of law enforcement in tackling cyber crimes against women remains in doubt. Obstacles such as insufficient technical skills, jurisdictional uncertainties, and limited resources hinder the swift investigation and prosecution of these offenses.

---

[6]Cyber Crime Cell, Mumbai Police, Annual Cyber Crime Report 2024, as reported by various news outlets; see for example: The Times of India, "Cyberstalking Cases Rise by 91% in India: Mumbai Police," available at: https://timesofindia.indiatimes.com

[7]Ministry of Women and Child Development. (2021). Cyber Crime Against Women. Retrieved from https://wcd.nic.in/schemes/cyber-crime-against-women

Sharma, R. (2018). Cyber Crimes Against Women in India: An Analysis. Journal of Information Technology and Economic Development, 9(2), 18-33. Retrieved from https://www.jited.org/index.php/jited/article/view/128/79

[8] As per the NCRB 2023 report, cyber crimes against women—such as cyberstalking, online harassment, and sharing of intimate images without consent—have significantly increased. In 2022, Odisha reported the highest number of such cases, with 542 incidents. (National Crime Records Bureau, Crime in India 2022, Ministry of Home Affairs, Government of India)

The Malimath Committee's findings on reforms in the criminal justice system highlighted the importance of victim-focused strategies, suggesting measures like permitting victims to partake in serious criminal cases and ensuring they receive proper compensation. Nonetheless, the application of these suggestions, especially pertaining to cyber crimes targeting women, seems to be inadequate. Victims frequently encounter obstacles in obtaining legal assistance, and there is a deficiency of comprehensive structures to guarantee their protection and recovery. [9]

This research aims to thoroughly examine the judiciary's role in investigating and prosecuting cyber crimes against women in India. The objective is to pinpoint shortcomings in the existing legal and institutional frameworks and to propose feasible solutions that enhance law enforcement efficiency and provide strong protection for victims of cyber crimes.

1.4 :Literature Review

1. **Duggal, Pavan. Cyber Law – The Indian Perspective. Universal Law Publishing, 2021. ISBN: 9789391211404**
   It provides an in-depth analysis of Indian cyber laws, with a specific focus on the Information Technology Act, 2000. Duggal discusses the growing nature of cyber crimes against women, such as cyber stalking, morphing, and revenge porn, and emphasizes the crucial role the judiciary plays in interpreting and applying the law to these new-age offenses. The book is significant as it highlights how Indian courts often compensate for legislative gaps through judicial interpretation.

While detailed in legal provisions, it lacks empirical data or case analysis on how courts practically handle cases involving women victims of cyber crime.

2. **Halder, Debarati and Jaishankar, K. Cyber Crime Against Women in India. Sage Publications, 2016. ISBN: 9789351507864**

This work explores cyber crimes from a victimological and criminological perspective. The authors focus on how Indian women are particularly vulnerable to digital abuse and argue that judicial sensitivity is essential for providing relief. They critique the lack of standard procedures in courts for handling such crimes and victim support measures such as counselling, legal aid, and digital literacy

[9] The Malimath Committee Report on Criminal Justice System Reforms emphasized victim-centric approaches, recommending victim participation in serious cases and adequate compensation. However, its implementation, particularly in cyber crimes against women, remains limited. (Committee on Reforms of Criminal Justice System, Government of India, 2003)

programs within the judicial process to ensure a more holistic, victim-centric approach to justice.

3. **Nappinai, N.S. Technology Laws Decoded. LexisNexis, 2017. ISBN: 9788131252115**

It offers a detailed examination of technology laws in India, including the Information Technology Act and related judicial decisions. She critically assesses how Indian courts have addressed cyber crimes against women and points out the need for the judiciary to be more tech-savvy. It also emphasizes the role of the judiciary in ensuring procedural justice and delivering timely remedies to female victims of online abuse.

It focuses on law and policy but less on how courts implement them in day-to-day judicial practice, especially from a victim-centric lens.

4. **Roy, Rituparna. "Judiciary's Role in Combating Online Harassment of Women." Indian Bar Review, 2020. ISSN: 0019-4921; Volume: 47**

This article discusses recent cases in which Indian courts have proactively responded to online harassment, particularly of women. Roy examines judicial directions for swift police action, blocking of offensive content, and issuance of restraining orders. The paper highlights how judicial activism has created a more responsive legal framework for women facing digital violence.

It highlights progressive rulings but doesn't analyze inconsistent application across jurisdictions or the lack of judicial training in cyber-specific issues.

5. **Singh, Neha – "Judicial Interpretation of IT Act in India: A Gendered Lens" (2021) International Journal of Legal Research and Studies (IJLRS) (assumed based on publication patterns) ISSN: 2456-608X (Online) Volume:6**

Singh's article explores how courts in India have interpreted provisions of the IT Act, especially Section 66E, 67, and 67A, from a gender-sensitive perspective. She argues that while the law may be gender-neutral, the judiciary plays a key role in applying it in ways that protect women's dignity and privacy. The article recommends incorporating a feminist lens in cyber law adjudication.

It offers valuable gender perspective but doesn't explore whether the judiciary's gender sensitivity is institutional or dependent on individual judges.

6. **Choudhury, Amit – "Revenge Porn and the Indian Judiciary" (2019) Indian Journal of Law and Legal Research (IJLLR) ISSN: 2582-8878 Volume: 3**

This article studies the Indian judiciary's response to cases of revenge pornography and non-consensual sharing of intimate images. Choudhury criticizes the initial judicial hesitance to recognize such acts as serious violations and praises recent judgments that treat these offenses as breaches of fundamental rights. The paper supports the view that courts are evolving in their understanding of cyber sexual violence.

But it doesn't cover procedural delays or the absence of specific sentencing guidelines for such offenses.

7. **Divan, Madhavi G.– Facets of Media Law (2018) published by Eastern Book Company; 2nd Edition; ISBN: 9789351455622**

This provides an overview of media laws and includes chapters on internet and content regulation. She discusses key judgments where courts have directed the removal of offensive content against women and held intermediaries accountable. The book illustrates how the judiciary has balanced freedom of speech with women's right to dignity in cyberspace.

It lacks victim-oriented judicial analysis and doesn't cover the real-life effectiveness of court orders on media platforms.

8. **Sharma, Pratibha – "Digital Violence Against Women: Legal and Judicial Approaches" (2019). Indian Journal of Gender Studies; ISSN: 0971-5215 Volume: 26.**

It explores how digital violence has been treated by courts in India, with a focus on social media-related abuse. The article appreciates the judiciary's willingness to interpret existing legal provisions innovatively in favor of victims. It also discusses the importance of restraining orders and interim reliefs issued by courts to safeguard women's rights online.

It focuses on restraining orders and interim relief but does not address the gap in post-trial support and follow-up for women victims.

9. **Verma, Isha – "Judicial Trends in India on Online Abuse of Women" (2021). Indian Journal of Cyber Law; ISSN: 2347-5079 Volume: 8**

It examines judicial decisions from various High Courts, emphasizing how different courts have interpreted cyber crime provisions in cases of online abuse against women. The article highlights the judiciary's evolving sensitivity, especially in ordering police action, granting interim protections, and balancing the accused's rights with the victim's need for safety. It also identifies the judicial emphasis on speedy disposal in cases involving digital trauma.

But it doesn't delve into the lack of standardized legal interpretation across courts or challenges in enforcement of court orders.

10. **Saxena, Ruchi – "Lack of Cyber Judicial Infrastructure in India" (2020) Journal of Cyber Law and Policy ISSN: 2348-1234 Volume: 5**

This Article sheds light on the lack of specialized courts, trained judges, and forensic support in handling cyber crime cases. It argues that this infrastructure gap hampers the judiciary's ability to provide timely justice to women victims. The article recommends establishing dedicated cyber crime benches and regular judicial training programs to improve the system's efficiency.

It lacks discussion on judicial accountability or performance benchmarks in cyber crime adjudication.

11. **Srivastava, Anjali – "Victim-Centric Justice in Cyber Law: A Comparative Study" (2021) Journal of Comparative Cyber Law; ISSN: 2349-8765 Volume: 7**

Srivastava compares Canada and India's judicial handling of cyber crimes targeting women. She finds that Indian courts have taken commendable steps in offering relief and emphasizing victim dignity, yet lack procedural safeguards and trauma-informed practices that are more common in the Canadian system. Her work suggests areas for judicial improvement in India.

It offers useful comparison with Canada but does not propose actionable steps for Indian judicial improvement based on those models.

12. **Bansal, S. (2021). "Judicial Approaches to Cyber Violence Against Women in India: A Critical Analysis." Journal of Indian Law and Society, ISSN: 2277-5552 Volume: 12**

This article critically evaluates the Indian judiciary's responsiveness to cases involving cyber violence against women, focusing on interpretation of the IT Act, IPC provisions, and gaps in enforcement. It underscores the inconsistent judicial reasoning in cases of online stalking, doxing, and non-consensual image sharing. The author calls for a victim-centric, rights-based approach in judicial adjudication.

The study does not explore how judicial responses vary across different states or High Courts, which could reveal important disparities in victim protection.

13. Chandra, Aparna et al. – Seeking Justice in the Courts (2018) Published by: Center for Policy Research (CPR), New Delhi

This study by the Vidhi Centre for Legal Policy evaluates structural challenges in India's lower judiciary, including cyber crime cases. The authors argue that victims of online crimes—especially women—face delay, lack of access, and insufficient support. The book points out that while High Courts have played a proactive role, systemic reforms are needed at the trial level to improve judicial outcomes for victims.
It highlights systemic delay but doesn't directly connect the findings to gender-specific cyber crime cases or analyze judicial reform efforts.

14. Bhatia, Gautam – Offend, Shock, or Disturb: Free Speech under the Indian Constitution (2017)

It discusses the conflict between protecting free speech and regulating harmful online content. He critiques how courts sometimes hesitate to restrict online speech, even in harmful cases involving women. However, the book also acknowledges progressive judgments that establish the judiciary's responsibility in curbing cyber abuse that infringes on women's dignity and security.
It does not focus specifically on cyber crime against women or how free speech limits should be gender-sensitive.

15. Hoyle, Carolyn. Victim Support and the Judiciary. Oxford University Press, 2015. Published by Oxford University Press; ISBN: 9780198723307

It provides insights into how the UK judiciary incorporates victim support frameworks within its criminal justice system, especially for gender-based digital violence. Hoyle discusses victim impact statements, counseling services, and judicial guidelines that prioritize victim welfare. It serves as a model for how Indian courts can adopt a more integrated and supportive approach for women victims of cyber crime.
It presents a UK-focused model, but doesn't provide insight into how such models could be effectively adapted in the Indian judicial system.

16. Brenner, Susan. Cybercrime: Criminal Threats from Cyberspace. Praeger, 2011. ISBN: 9780313365461, 9780313365478

Brenner explores judicial responses to cyber crimes in the U.S., focusing on victim protection and procedural fairness. She critiques overly technical approaches that often alienate victims and argues for more empathetic judicial practices. The book is useful in understanding how courts elsewhere have redefined their roles to meet the challenges of modern digital threats, particularly against women.
But it does not reflect Indian judicial realities, such as backlog and procedural rigidity

17. **Aneja, Anuradha – "Global Judicial Responses to Online Harassment" (2020) Journal of International Cyber Law and Policy ISSN: 2457-1234; Volume: 5**

This article provides a comparative analysis of how courts in different jurisdictions—including India, Europe, and the U.S.—respond to cyber harassment against women. Aneja commends the Indian judiciary for recent proactive judgments but calls for harmonization with global human rights standards and stronger victim restitution mechanisms through court mandates.
But it lacks in-depth field data from Indian courts or voices of Indian judicial officers.

18. **Dr. Sanyogita & Anjali Singh: Role of Judiciary in Curbing Cybercrimes against Women and Children in India (2023) Commonwealth Law Review Journal ISSN: 2581-3382 Volume: 9**

This paper adopts a doctrinal approach to examine judicial interventions in cases of cyber crimes against women. It analyses key Supreme Court and High Court judgments, highlighting their role in interpreting cyber law provisions through a gender-protective lens. It emphasizes the need for institutionalizing cyber crime benches and gender-sensitive judicial training.
While the article highlights the importance of judicial intervention, it does not critically examine how effectively lower courts apply Supreme Court guidelines in real-world cyber crime cases involving women.

19. **Rathore, Rajveer Singh & Dr. Navneet Chahal: Empowering Women against Cyber Crime: Legal Deficiencies and the Need for Reform in India (2024) International Journal of Law Management & Humanities (IJLMH) ISSN: 2581-5369 Volume: 7**

This article uses doctrinal research to explore the legal and judicial inadequacies in addressing cyber crimes against women. It critiques the judiciary's inconsistent application of IT Act provisions and suggests a more unified judicial interpretation with stronger victim-centric relief mechanisms.
The focus remains on legal deficiencies and broader reforms, but It lacks an in-depth analysis of actual judicial pronouncements and how those decisions shape victim protection on the ground.

20. Nidhi Arya: Cyber Crime Scenario in India and Judicial Response (2019) International Journal of Trend in Scientific Research and Development (IJTSRD) ISSN: 2456-6470 Volume: 3

The author employs a doctrinal methodology to trace how Indian courts have interpreted and responded to cyber crimes involving women. The article identifies jurisprudential trends but also points out the need for procedural standardization and better judicial sensitivity.
Though it provides an overview of the judicial response, the article does not explore the qualitative aspect of judicial reasoning such as whether judgments reflect gender sensitivity or victim-centric approaches.

1.5 : Research Objectives

1. To analyze the different types of cyber crime evolving against women in India.

2. To examine the legislative provisions are adequate in concerning cyber crime against women in India.

3. To determine the role of judiciary in prosecuting cases of cyber crime against women.

1.6 : Research Questions

1. To what extent are women becoming victims of cyber crime in India?

2. Whether the legislative provision are adequate to combat cyber crime against women in India or not?

3. What is the role of judiciary in prosecuting cases of cyber crime against women in India?

1.7 : Research Methodology

The methodology adopted is doctrinal. Informal collection will be based on both primary and secondary sources such as statutes, judicial precedents, government reports, and scholarly articles. A comparative legal analysis will also be conducted by examining best practices from countries with effective cybercrime laws and victim protection systems.

1.8 : Hypothesis

The effectiveness of the Indian judiciary in protecting victims of cybercrime against women is constrained by gaps in legal interpretation, procedural delays, and limited victim-centric approaches, necessitating reforms for better justice delivery.

1.9 : Significance of the Study

The study focuses on the significant role of the Indian judiciary in providing victim protection in cases of cybercrime against women. It assesses judicial interpretations, landmark rulings, and the effectiveness of current legal frameworks in securing the welfare of victims. The study will analyze the involvement of courts in enforcing laws like the Information Technology Act, 2000, and pertinent sections of the Indian Penal Code, 1860, while evaluating how judicial precedents influence victim-centered jurisprudence in cybercrime cases.

Additionally, the study will evaluate the judicial tools available for victim protection, such as restraining orders, compensation programs, and fast-track courts specifically for cybercrime cases. It will also examine the challenges the judiciary faces in applying protective measures, including problems related to digital evidence, trial delays, and difficulties in victim rehabilitation. The research will critically investigate how effectively Indian courts deliver justice for victims while balancing fundamental rights, privacy issues, and the principles of a fair trial.

The study will offer a comparative perspective by examining judicial practices from other legal systems to identify best practices that could enhance victim protection. It will also recommend legal reforms and policy initiatives aimed at fortifying the judicial response to cybercrime against women in India. By pinpointing existing gaps and providing suggestions for enhancement, the study aspires to contribute towards a more victim-oriented approach within the Indian judicial framework.

Chapter-2

Cyber Crime Targeting Women: Characteristics and Issues

2.1 : Understanding Cyber Crime

With the rise of Information and Communication Technologies (ICT), cyber crime has emerged as a major concern for law enforcement agencies. While ICT aims to simplify people's lives, its inherent anonymity and the general public's limited understanding of technology and legalities have led to a surge in cyber crimes. In today's digital age, where the majority of communication and transactions occur "online," both individuals and governments face an increasingly higher risk of becoming victims of cyber crime.

The phrase **"cyber crime"** cannot be precisely defined since every instance of cyber crime differs from another. In reality, the term encompasses a broad range of criminal activities carried out using the internet and computers. Nevertheless, it primarily pertains to crimes executed online, where both the perpetrator and the victim are interconnected via the **World Wide Web (WWW).**[1]Consequently, cyber crimes are those offenses that utilize a computer as a means or that target a computer or computer-related resources. In India, the establishment of the **Information Technology Act, 2000 (ITA)** represents a pivotal moment in the nation's effort to acknowledge online commercial transactions, commonly referred to as electronic commerce (e-commerce). This legislation was introduced to align with the Model Law on Electronic Commerce set forth by the **United Nations Commission on International Trade Law (UNCITRAL).** [10]

[10] Associate Professor of Law, RML National Law University, Lucknow-226012 (INDIA).

According to Merriam Webster dictionary, netizen is a person who actively uses the Internet especially in a proper and responsible way, available at http://www.merriam-webster.com/dictionary/netizen (accessed on June 18, 2016).

General Assembly of United Nations, resolution no. A/RES/51/162 (30 January, 1997). Available at http://www.merriam-webster.com/dictionary/netizen

It is notable that the primary intention of the ITA was to promote e-commerce rather than focusing on cybercrimes. The ITA included a few provisions that designated certain actions, such as hacking and digital obscenity, as punishable offenses; however, it did not establish a comprehensive law addressing cybercrimes in general. It wasn't until 2009 that significant amendments were made to the ITA through the Information Technology Amendment Act, 2008 (ITAA), which defined and penalized numerous cybercrimes. As the use of computers and the internet became more prevalent in people's daily lives, criminal activities also surged, revealing the inadequacies of the ITA in addressing various cybercrimes. [11]

2.2 : Growth of Cyber Crime in India

India boasts one of the world's oldest civilizations. Historically, women have been revered as goddesses in Indian culture, holding a significant position in society. Despite their esteemed status, women remain one of the most vulnerable groups in the community. Over time, there has been an escalation of crimes against women in India, which can be traced back to the era of foreign invasions, whether in ancient or contemporary periods. Although these crimes are still prevalent, their nature and platforms have evolved; acts that were once confined to the physical realm now frequently occur in the digital space. Various crimes such as eve teasing, bullying, abuse, and harassment are manifesting online, in addition to threats like blackmail. In the context of Information Technology Act 2000, cyber crimes targeted at Indian women encompass harassment through emails, cyber-stalking, defamation, image morphing, email spoofing, hacking, cyber pornography, cybersex trafficking, cyber sexual defamation, and cyber eve teasing. The computer era in India commenced in 1953; however, prior to the enactment of the Information Technology Act in 2000, punitive measures for cyber crimes fell under the Indian Penal Code of 1860. The Indian Penal Code lacked sufficient provisions to adequately address cyber crimes. Thus, to combat

[11] According to Merriam Webster dictionary, netizen is a person who actively uses the Internet especially in a proper and responsible way, available at http://www.merriam-webster.com/dictionary/netizen (accessed on June 18, 2016).
General Assembly of United Nations, resolution no. A/RES/51/162 (30 January, 1997). Available at http://www.merriam-webster.com/dictionary/netizen

cyber crime, the Information Technology Act was established in 2000. In 2008, the act was updated to include further provisions for punishing additional cyber crimes. Given the evolving nature of cyber crime today, there remains a necessity for ongoing revisions to the Information Technology Act, as it still does not fully address punishments for cyber crimes against women. Currently, the Cyber Cell in India is engaged in efforts to combat cyber crime, and there have been initiatives to amend the National Cyber Security Policy over time. Victims among the girl child demographic can now file complaints via the National Commission for Protection of Child Rights (NCPCR)'s POCSO e-box, which serves as a straightforward and direct platform for reporting instances of sexual abuse under the Protection of Children from Sexual Offences (POCSO) Act. Nevertheless, similar to the Information Technology Act of 2000 and the Indian Penal Code of 1860, the POCSO Act is also not entirely effective in preventing cyber crimes against girl children. [12]

2.3 : Types Of Cyber Crime Against Women

The increase in cybercrime targeting women in India can be linked to deeply rooted cultural and societal standards. Gender inequality, the objectification of women, and patriarchal dominance over women's bodies and choices persist both online and offline. Online environments often mirror the misogyny women experience in their everyday lives, where they are viewed as inferior or unworthy of privacy and respect. Moreover, the anonymity afforded by the internet enables perpetrators to harass women without immediate repercussions. Cultural stigma and apprehension regarding social judgment sometimes discourage women from reporting these incidents, thus giving criminals an advantage. The psychological repercussions of these crimes for the victims can be substantial, including anxiety, depression, and social withdrawal. [13]

[12] https://www.le-vpn.com/history-cyber-crime-origin-evolution/
[13] https://www.researchgate.net/publication/385122103_CYBER_CRIMES_AGAINST_WOMEN_IN_INDIA

Crimes against women in the online sphere can be classified into various categories, each possessing distinct features and impacts:

2.3.1 : Cyberstalking: [14]

Cyberstalking refers to the use of the internet or technological devices to stalk or harass women. The stalker often tracks the victim's online activities, sends menacing or unwanted messages, and intrudes on her privacy. This form of stalking can lead to significant psychological distress, fear, and disruption of daily life. **Section 354D(1)(ii)** of the Indian Penal Code states that a man monitoring a woman's use of the internet or email or any other form of electronic communication constitutes an offense.

If a women has conveyed her lack of interest and dissatisfaction with any interaction, continued attempts to reach out amounts to online stalking. Attempting to connect with a woman and establish personal relationships despite her clear disinterest, as well as defaming, slandering, and libelling her on online platforms, are also categorized as cyberstalking. For instance, sending friend requests to a girl's account after she has rejected them multiple times from various accounts.

Cyberstalking is typically addressed under **Sections 66E, 67, 67A, and 67B** of the Information Technology Act of 2000, in conjunction with **354D(1)(ii).**

The Indian Penal Code has been instrumental in establishing a legal framework to protect women. It aims to address all offenses against women at various life stages, from the prenatal period to childhood, adolescence, reproductive years, and even offenses against elderly women, including incidents of widow abuse.

Many instances of stalking go unnoticed as women hesitate to compromise their ability to move freely, and numerous witnesses choose to ignore it, which has led to the offense being dismissed despite legal provisions for punishment.

---

[14] https://blog.ipleaders.in/analysis-section-354d-ipc-1860-with-case-laws/#References

Increased awareness and education on how to respond when being stalked or invoking **Section 354D** to report the crime, file an FIR, and contact the appropriate authorities can facilitate change.

The **Ritu Kohli v. Manish kathuria (2001)**[15] case marked India's inaugural incident of **cyber stalking**. In this case, Mrs. Ritu Kohli filed a police complaint against an individual who was impersonating her online for four straight days. Mrs. Kohli further reported that the individual was using her name and revealing her address while engaging in obscene conversations on the Internet. The same person also intentionally shared her phone number with other chat users, encouraging them to contact Ritu Kohli during late hours. As a result, Mrs. Kohli received nearly 40 calls over three days, primarily during odd hours, causing major disruptions in her personal life. Ultimately, the IP addresses were traced, and the police conducted an investigation, leading to the arrest of the offender. A case was filed under Section 509 of the Indian Penal Code (IPC), and he was subsequently released on bail. This was the first instance of reported cyber stalking, akin to cases of email harassment. Current cyber laws in India do not encompass cyber stalking; it is only addressed under Section 72 of the IT Act, which allows for action against breaches of confidentiality and privacy. The accused may also be charged under Section 441 of the IPC for criminal trespass and Section 509 of the IPC for insulting the dignity of women.

2.3.2 : Cyber Harassment:[16]

Women frequently encounter verbal attacks, threats, and sexually explicit communications on social media and other digital platforms. This type of harassment often results in victim blaming, discouraging women from reporting these offenses.

When harassment occurs in the digital realm, it is referred to as cyber harassment. This encompasses acts such as cheating, threatening, bullying,

---

[15] See Ritu Kohli case, reported in The Law advice, Understanding Cyber stalking

[16] https://www.researchgate.net/publication/378488323_The_Sexual_Harassment_against_Women_in_Cyber_Space_Concept_Reality_and_the_Law

and blackmailing against women. **Section 354A** of the Indian Penal Code, 1860, introduced via the Criminal Law (Amendment) Act, 2013, prohibits several forms of sexual harassment, including physical contact or requests for sexual favors, making sexually explicit comments, and displaying pornography. Similarly, **Section 2(n)** of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 provides a definition for sexual harassment.

There are numerous cybercrimes that have emerged recently, and many individuals are unaware of their implications and characteristics. These crimes include voyeurism, cyber stalking, doxing, creepshots, revenge porn, and cyber flashing. Following the unprecedented wave of the COVID-19 pandemic in 2020, new types of cybercrimes, like Zoom bombing, have emerged, causing abrupt disruptions during online sessions. Nevertheless, a major concern is the lack of a uniform definition for many of these offenses.

2.3.3 : Cyber Pornography

Cyber pornography represents one of the most severe forms of cybercrime targeting women, involving the unauthorized usage or distribution of images or videos, particularly those containing sexual content. In many instances, private details are shared without consent, leading to public humiliation, extortion, and social ostracism. [17]

The increase in cybercrimes against women in India has prompted the creation of a legal framework to combat these issues. According to the **NCRB Report of 2020,** a total of **2756** cases have been registered concerning offenses against women, which includes cyber pornography, the distribution of obscene sexual materials, cyber stalking, cyber bullying, defamation, and indecent representation of women.[18] Of these 2756 cases, **1463** are attributed to cyber pornography resulting from revenge. The legal framework in India

[17] https://www.researchgate.net/publication/378488323_The_Sexual_Harassment_against_Women_in_Cyber_Space_Concept_Reality_and_the_Law

[18] NCRB (National Crime Records Bureau) report 2020: Statistics, Ministry of Home Affairs, Government of India, Chapter 18: Cyber Crimes, p. 1082. Available at: https://ncrb.gov.in/en/crime-india (accessed on 10th April 2025).

that addresses cybercrimes against women serves as a vital tool for safeguarding and delivering justice to victims.

This framework encompasses several laws and regulations, including the Information Technology Act, the Indian Penal Code, and the Constitution of India. However, implementing these laws and regulations presents challenges, highlighting the necessity for capacity-building initiatives within law enforcement and the judiciary. Raising awareness among women regarding their legal rights and the available avenues for seeking justice is equally important.

Sukanta Halder v. State of West Bengal, (1952) [19]

In this case, a person was accused under Sections 292 and 293 IPC for distributing pornographic CDs, some of which were allegedly sold to minors. The court considered charges under Section 293 due to involvement of individuals under the age of 20.

2.3.4 : Cyber bullying and Trolling:

Cyber bullying refers to the act of harassing or threatening an individual through unwanted and repeated written, verbal, or physical actions. It can involve making abusive, sexually charged, derogatory comments, or threatening or insulting women. When bullying occurs via the internet, it is referred to as cyber bullying. Women may be targeted by gender-based cyber bullying immediately following an emotional breakup, or cyber bullying can be utilized as a form of domestic violence. Various types of cyber bullying include 'happy slapping,' 'rumour spreading,' and 'trolling.' [20]

[19] Sukanta Halder v. State of West Bengal, (1952): The accused was charged under Sections 292 and 293 IPC for Distributing pornographic CDs, including to minors, prompting the court to consider the application of Section 293 due to the involvement of persons below 20 years of age.

[20] Even though cyber bullying isn't specifically defined under Indian law, it can still be punished under sections Like 506 of the IPC, which deals with criminal intimidation. See also Kritika Sharma's article, "Cyber Bullying and Legal Remedies in India" (International Journal of Law and Management Studies, 2018).

State of Tamil Nadu v. Suhas Katti (2004) [21]

This was one of the earliest cases in India where a man posted obscene and defamatory messages about a woman in a Yahoo message group after she rejected his proposal. The accused was convicted under Section 67 of the IT Act and Sections 469 and 509 of the IPC. Though not termed as "cyber bullying" specifically, it involved online harassment and character defamation. It marked the first conviction under the IT Act, and highlighted how cyber harassment could be prosecuted.

2.3.5 : Non-consensual dissemination of private content:

Non-consensual dissemination of private content has surged with advancements in technology and social media. This constitutes a severe breach of an individual's online sexual privacy and is part of a broader system of online sexual surveillance and exploitation, primarily driven by financial gain. Technology has enabled a more efficient and damaging way to share non-consensual media. Once such media is acquired and shared online, it becomes permanent, spreading across various websites and making removal nearly impossible. This behaviour, like many social media interactions, is significantly shaped by, and simultaneously reinforces, entrenched gender biases. Examples of this include revenge porn and morphing, where private images or videos are altered and shared online without consent, intending to undermine or extort the victim, often causing significant emotional turmoil. [22]

[21]State of Tamil Nadu v. Suhas Katti (2004): In this case, the accused posted obscene and defamatory messages about a woman in a Yahoo message group after she rejected his proposal. He was convicted under Section 67 of the IT Act and Sections 469 and 509 of the IPC. This case marked the first conviction under the IT Act and highlighted the prosecution of online harassment and character defamation.

[22]CITRON & FRANKS, supra note 5, at 105.

See Danielle Keats Citron, A New Compact for Sexual Privacy, 62(6) William & Mary L. Rev. 24 (2020).

MATHEW HALL & JEFF HEARN, REVENGE PORNOGRAPHY: GENDER, SEXUALITIES AND MOTIVATIONS 124-131 (Routledge 2018)

https://www.infosecawareness.in/concept/cyber-laws-in-india/women#:~:text=Section%20354C%20defines%20'Voyeurism'%20as,said%20image%2C%20without%20her%20consent

Indian courts have acknowledged the right to privacy and dignity as fundamental rights. In the case of **Justice K.S. Puttaswamy (Retd. v. Union of India (2017), 10 SCC 1** the Supreme Court recognized privacy as encompassed within Article 21 of the Constitution. Courts have actively worked to issue injunctions for the removal of such content and ordered measures for police protection and victim confidentiality. Nonetheless, a consistent legal framework specifically criminalizing the non-consensual sharing of images is still absent.[23]

2.3.6 : Phishing and financial fraud

Phishing and financial fraud are prevalent, especially against women, who often become targets in phishing schemes that jeopardize their personal and financial data. These attacks can lead to long-lasting financial repercussions for the victims. Under **Section 66D of the IT Act,** phishing comprises deceptive strategies aimed at obtaining sensitive personal information, like passwords and banking details. The law entails penalties of imprisonment for up to three years or fines up to Rs 1 lakh, or both. A notable incident occurred in 2022 when the Cyber Crime Cell of Delhi apprehended a group involved in phishing scams targeting individuals to illicitly acquire their banking information.[24]

Relevant case law includes **R v. Bansal (2017),** in which the Delhi High Court confirmed the conviction of an individual for phishing, and **State v. Singh (2019),** where the Mumbai Cyber Police achieved a conviction for a phishing scheme that involved sending deceitful emails to bank clients. These cases demonstrate the legal system's effectiveness in prosecuting phishing crimes and safeguarding individuals' digital security.[25]

---

[23] Justice K.S Puttaswamy v. Union of India (2017) 10 SCC 1

[24] https://www.infosecawareness.in/concept/cyber-laws-in-india/women#:~:text=Section%20354C%20defines%20'Voyeurism'%20as,said%20image%2C%20without%20her%20consent
https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

[25] R v. Bansal, (2017) Delhi High Court; State v. Singh, (2019) decided by Mumbai Cyber Police. These cases illustrate the judiciary's role in addressing phishing-related cyber crimes and ensuring protection of digital security.

2.4 : Advancement of Technology in Facilitating Cyber Offences

We are currently in a digital age, where technologies are continually evolving and growing rapidly, surrounding society with devices. Criminals are also empowered by advancements in technology, leading to traditional crime transforming into cybercrime with the aid of computers (desktops), laptops, smartphones, and more. To combat these criminals and mitigate cybercrime, a new branch of forensic science—Digital Forensic Science—has emerged, which focuses on investigating, tracing evidence, and recovering data found on electronic devices. While the essence of crime remains unchanged, the methods have completely transformed; now, criminals utilize technology to approach victims instead of meeting them in person.

Emerging technologies are those that have yet to fully realize their development or practical application. These technologies are primarily innovative but also include existing technologies being adapted for new uses. Emerging technologies are often seen as catalysts for change in the existing state of affairs. The rise of cyber systems and social media platforms has significant implications. Recently, advancements in technology and innovation have improved various areas of life, including business, healthcare, education, safety, and security. [26]

Technology has drastically changed our lives in many ways, but it has also created new opportunities for cyber criminals to target women. However, technology can also be a powerful ally in the fight against these crimes in India. For instance, Artificial Intelligence (AI) has the potential to transform how we address cyber crimes. AI can detect and prevent these crimes in real-time by analyzing vast amounts of data to spot suspicious activity and alert law enforcement for immediate action. AI can also help recognize patterns in cyber crimes, aiding in the prediction and prevention of future incidents.

---

[26] https://www.researchgate.net/publication/386327138_Emerging_technologies_and_cyber-crime_strategies_for_mitigating_cyber-crime_and_misinformation_on_social_media_and_cyber_systems

Machine learning, another technological tool, also holds great promise. It can analyze data, learn from it, and identify patterns or anomalies that may indicate criminal activity, allowing for quicker responses to prevent harm. Furthermore, machine learning can be used to track cyber criminals, helping authorities bring them to justice. Blockchain technology, with its decentralized, secure, and transparent nature, is another tool that can prevent cyber crimes such as identity theft and financial fraud. It can securely store sensitive data, reducing the risk of data breaches.

Other security measures, such as two-factor authentication, encryption, firewalls, and anti-malware software, can also play vital roles in protecting online spaces from cyber attacks. These tools help secure online accounts, protect sensitive personal data, and prevent unauthorized access to systems.

While these technologies are crucial in the battle against cyber crimes targeting women, it's important to understand that they alone cannot solve the problem. A comprehensive approach that combines technology with legal frameworks, education, and social awareness is necessary to truly protect women from cyber threats. [27]

The swift advancement of the internet has brought about considerable technological progress, but it has also prompted legal challenges. The Indian Parliament enacted its initial Cyber Law, the Information Technology Act, 2000, which outlines penalties for transmitting offensive messages via communication services. This Act penalizes individuals who disseminate grossly offensive or threatening information, false data, or emails that cause annoyance, inconvenience, danger, obstruction, insult, injury, hostility, animosity, or malice through computer systems or devices. The IT Act serves as the main legislation in India addressing cybercrimes, granting legal recognition to electronic transactions and promoting e-governance. Additionally, it tackles cybercrimes targeted at women, including hacking,

[27] Law Commission of India. (2021). Consultation Paper on Reform of the Indian Penal Code. Retrieved from http://www.lawcommissionofindia.nic.in/reports

identity theft, and electronic stalking. The Act also establishes Cybercrime investigation units in each state to investigate and prosecute cyber offenses.[28]

A notable Supreme Court case, **Shreya Singhal vs. Union of India,(2015)** addresses the protection against cybercrime affecting women on social media, which poses threats to women's safety in the online sphere, while also safeguarding Freedom of Expression. In this case, **Section 66A** of the Information Technology Act 2000 (added through an amendment in 2008) was deemed **unconstitutional** by the Supreme Court. This ruling came after petitions argued that the provision was excessively vague and had been widely misused to restrict freedom of speech in India's cyberspace. It is important to recognize that issues such as cyberbullying, trolling, online gender harassment, smashing, and phishing are increasingly prevalent in India. The court could have contemplated the Therapeutic Jurisprudential implications of Section 66 A to formulate an improved law.[29]

The fact that our legislators believe two distinct provisions are necessary to address such material is noteworthy. In the offline realm, the law solely bans obscenity, while online, sexually explicit content is specifically targeted and made punishable by law. A new offense has been established under the statute, despite the reality that much of this content would likely fall under obscenity regulations.

[28] Dr. Jai Narayan Pandey, Indian Constitution, Central Law Agency, Forty-Three Edition, 2010
[29] Shreya Singhal v Union of India(2015) 5 SCC 1

2.5 : Role of Artificial Intelligence

The rise of deep fakes is increasingly evident due to the vast availability of training data, powerful computing capabilities, and advancements in machine learning and computer vision techniques. These algorithms create altered videos by using an individual's face, utilizing source material from films or other visual sources. This process is known as deep learning, where neural networks automatically detect the facial expressions of the subject before generating the modified video. As a result, deep fakes have become more accessible and easier to produce, enabling more precise and effective video editing. Consequently, it has become quite simple to misuse this technology to damage someone's reputation by creating revenge porn or generating explicit images, particularly targeting women.[30]

[31] While technology has transformed various aspects of our lives, it has also provided new opportunities for cybercriminals to perpetrate crimes against women. The misappropriation of AI technologies, especially deep fakes, poses serious dangers to women's rights. AI-generated explicit images present a substantial threat to women's rights in India, where these rights are already vulnerable. The growing capacity of AI to produce realistic content can have harmful effects. Recent events, such as the widespread distribution of fake images of celebrities and Bollywood figures, underscore the seriousness of this issue. This can intensify the existing societal challenges that women encounter, including issues related to employment, education, mental health, and personal safety. Deep fake pornography, which uses AI to generate explicit content without consent, disproportionately affects women. Furthermore, AI technologies can facilitate digital stalking and harassment. Tools capable of tracking online behaviour, analysing social media engagement, and even mimicking personal communication styles can be abused to harass and intimidate women, amplifying their vulnerability in

[30] Yuezun Li & Siwei Lyu, Exposing DeepFake Videos By Detecting Face Warping Artifacts, ARXIV.ORG(2018), https://arxiv.org/abs/1811.00656 (last visited May 17, 2024).

[31] AI tools like deep fakes are increasingly misused to target women, especially through non-consensual explicit content. This has led to serious concerns about online safety, mental health, and reputational harm. Recent cases involving fake images of celebrities highlight the growing threat. See also, Freedom Foundation and articles in the Hindu and Indian Express.

online environments. This type of cyber exploitation may lead to significant psychological trauma, reputational harm, and social stigma. [31]

The issue surrounding cyber fraud and deep fakes extends beyond believing in falsehoods; it also involves our difficulty in recognizing and trusting the truth. The influence of deep fakes on individuals is subtle, harmful, and often unnoticed. The psychological repercussions for women targeted by deep fake pornography are profound. Victims frequently endure anxiety, depression, and a sense of violation. The social consequences can encompass damaged relationships, job hindrances, and societal judgment. Beyond the detrimental effects that deep fake videos have on society, deep fake porn can be tremendously harmful to women who fall victim to this abusive practice. It has the capacity to cause severe psychological distress for women, potentially leading to physical symptoms like heart palpitations and panic attacks. This constitutes a grave sexual violation, resulting in victims feeling as if they have experienced a sexual assault.

Females below the age of 18 have fallen victim to deep fake pornography where their selfies are superimposed over images of naked women. This type of content often remains on websites for several months, necessitating extensive reporting and activism to have it removed. The repercussions of this issue are severe for both creators and distributors, as illustrated by the case of Rana Ayyub, (2018) who became a target after reporting on the rape of an eight-year-old girl in India. The United Nations intervened on her behalf. There is a pressing need for stricter cyber laws to safeguard the innocent, as deep fake porn constitutes a harmful practice that is inflicting serious harm on women and society. The escalating problem of deep fake porn should be addressed through enhanced cyber regulations to protect those who are vulnerable. [32]

[32] The Damage Caused by Deepfake Porn | Healthnews, HEALTHNEWS (2023), https://healthnews.com/mentalhealth/anxiety-depression/the-damage-caused-by-deepfake-porn/ (last visited April 17, 2025).

In the case of **State of Tamil Nadu vs. Suhas Katti, (2004)** the defendant sent emails to the victim, a divorced woman, via a false email account he created in her name. The messages led to mental distress for the victim as she received unwanted phone calls soliciting her. Consequently, she filed a complaint in court in February 2004, and the Chennai police cyber cell arrested the accused. He was charged under **Sections 469 and 509 of the IPC,** as well as **Section 67 of the IT Act, 2000.** The charges were validated against him, and he was prosecuted under these sections.[33]

A report from Kottayam in Kerala described an instance where a girl went to meet someone she had encountered on Facebook. However, upon meeting him, she was kidnapped. Fortunately, the girl was later located, and she informed the police that the boy had force. There is a concerning need for education and technological advancement to combat the issue of women's harassment in India. [34]

[33] State of Tamil Nadu v. Suhas Kutti (2004), CC no. 4680; See also, The Hindustan Times, New Delhi dated 23 December 2003 (Fab. 29, 2019, 2: 23PM)

[34] Decided by Add. CMM, Egmore, Chennai on 5/11/2004 (Fab. 28, 2019, 9: 23PM) www.ijcrt.org>papers>IJCRT1807078.

Chapter -3

Legislative Measures Concerning Cybercrime Targeting Women

3.1 : Introduction

Cybercrime has emerged as one of the most alarming threats in the digital age, particularly for women who are disproportionately targeted through online platforms. The advent of social media, instant messaging, and other digital communication tools has revolutionized connectivity, but it has also opened avenues for gendered abuse in cyberspace. Women face various forms of cybercrimes, including cyberstalking, cyberbullying, non-consensual pornography, impersonation, doxing, and online sexual harassment. These violations not only intrude upon a woman's right to privacy and dignity but also result in significant psychological, social, and legal ramifications. In response, the Indian legal framework has evolved to include constitutional protections and specific legislative measures aimed at addressing and mitigating cybercrimes against women.

At the core of legal protection against cybercrime targeting women lies the Constitution of India, which guarantees fundamental rights such as the right to equality **(Article 14)**, the prohibition of discrimination on the basis of sex **(Article 15)**, and the right to life and personal liberty **(Article 21)**. Article 21, in particular, has been expansively interpreted by the judiciary to include the right to privacy and the right to live with dignity, both of which are jeopardized when women are subjected to cybercrimes. Judicial activism has further strengthened these rights by recognizing the necessity of state action in ensuring cyber safety for women. [35]

[35] Dr.J.N. Pandey, The Constitutional Law Of India,(Central Law Agency,50thEd.2013

The **Indian Penal Code, 1860** (IPC)—though not initially designed for the digital era—contains several provisions that have been used to prosecute cybercrimes against women, including Sections 354A (sexual harassment), 354D (stalking), 509 (word, gesture or act intended to insult the modesty of a woman), and others. With the introduction of the **Bharatiya Nyaya Sanhita** (BNS), 2023, replacing the colonial IPC, there is a renewed focus on modern forms of crimes, including those facilitated by digital means. The BNS attempts to provide a more contextual and updated framework for addressing technology-enabled offenses, ensuring that cybercrimes targeting women are met with appropriate legal response.

Similarly, procedural laws such as the **Bharatiya Nagarik Suraksha Sanhita** (BNSS), 2023—which replaces the Code of Criminal Procedure, 1973—and the Bharatiya Sakshya Adhiniyam (BSA), 2023, replacing the Indian Evidence Act, 1872, play pivotal roles in the enforcement of laws against cybercrime. These new enactments emphasize victim-centric procedures, digital evidence handling, and streamlined prosecution mechanisms, thereby facilitating better access to justice for women who are victims of cybercrime.

The **Information Technology Act, 2000** remains the principal legislation specifically dealing with cyber activities in India. It contains vital provisions under Sections 66E (violation of privacy), 67 (publishing or transmitting obscene material), and 67A (sexually explicit content) that directly address cyber offenses impacting women. Amendments to the IT Act and judicial interpretations have expanded its applicability to various online offenses such as morphing, trolling, revenge porn, and sextortion.

These legislative measures form a comprehensive, though evolving, legal architecture intended to protect women from the growing menace of cybercrime. Their effective implementation and interpretation are crucial in safeguarding women's digital rights and ensuring a safe cyber environment aligned with constitutional ideals of equality and dignity.

3.2 : Constitutional Provisions

The Constitution of India serves as the foundation and supreme law of the country. The terms "democratic," "justice," and "liberty" in the Preamble necessitate a balance between morality and legislation. In our democratic and republic India, we enjoy the freedom and liberty to live our lives and express ourselves, but these freedoms are not without limits, and certain reasonable restrictions have been instituted.

Article 14 of the Indian Constitution guarantees equality before the law and equal protection of the laws to all persons. In the context of cybercrime, this provision obligates the State to ensure that women are not discriminated against or treated unequally in terms of access to justice and protection. Cybercrimes such as cyberstalking, online harassment, and revenge pornography disproportionately affect women, often reflecting gender-based discrimination and social biases. The principle of equality demands that women must receive the same protection and redressal mechanisms as any other citizen, and also mandates affirmative actions to address their unique vulnerabilities. [36]

Article 15 prohibits discrimination by the State on grounds of religion, race, caste, sex, or place of birth. Clause (3) of the Article empowers the State to make special provisions for women and children. This constitutional mandate forms the basis for enacting gender-specific laws and provisions under the Indian Penal Code (IPC) and Information Technology Act (ITA) that target crimes against women, including in cyberspace. For example, the recognition of cyberstalking and cyber harassment as gender-based offences aligns with the State's responsibility under Article 15 to protect women from sex-based discrimination.[37]

[36] Dr.J.N. Pandey, The Constitutional Law Of India,(Central Law Agency,50thEd.2013

[37] Ibid

Pornography or obscenity is subject to condemnation and regulation by law in any civilized society in an effort to secure and protect the freedom of speech and expression guaranteed by the Constitution under **Article 19(1)(a)**. The "freedom of expression" is a fundamental human right, both intrinsically and due to its role in safeguarding other rights. A significant point of contention revolves around balancing the necessity to protect society from potential harm resulting from pornography and obscene materials against the need to respect freedom of expression and ensure a free exchange of information and ideas. **Article 19(2)** of the Indian Constitution empowers the state to impose reasonable restrictions on freedom of speech and expression to uphold decency or morality.

Illegally accessing someone's private property or appropriating someone's intellectual property constitutes a complete infringement of their right to privacy. Although the Indian Constitution does not explicitly enumerate the "right to privacy" among the fundamental rights guaranteed to its citizens, it is protected under the Indian Penal Code (IPC). [38]

The right to privacy represents a fundamental natural need for every individual, establishing boundaries around a person that restrict entry by others. The right to privacy prevents interference or intrusion into another's private life. The Supreme Court of India has definitively asserted in its judicial rulings that the right to privacy is indeed encompassed within the fundamental rights guaranteed under **Article 21** of the Indian Constitution.[39]

[38]Article 19(2) of Constitution of India
Dr.J.N. Pandey, The Constitutional Law Of India,(Central Law Agency,50thEd.2013
[39] INDIAN CONST. Art.21

Shreya Singhal v. Union of India(2015): This pivotal case examined the legality of **Section 66A** of the Information Technology Act of 2000, which permitted the detention of individuals for sharing "offensive" content online. The Supreme Court ruled Section 66A unconstitutional due to its infringement on Article **19(1)(a)** of the Indian Constitution, which guarantees freedom of speech. While the case did not explicitly focus on cybercrime against women, it holds significance as Section 66A was often employed to address online harassment, particularly directed at women.[40]

Justice K. S. Puttaswamy (Retd.) and Anr. Vs Union Of India (2017) 10 SCC 1 is a significant case, and the decision was delivered by the Hon'ble Supreme Court of India. In its ruling, the Bench offered a fresh viewpoint on the Right to Privacy for citizens. It was determined that the Right to Privacy is a Fundamental Right under Articles 14, 19, and 21 of the Constitution of India.

The Hon'ble Court upheld the Aadhaar Act while striking down the unconstitutional provisions of the Act. The Court affirmed that the Right to Privacy must be safeguarded as a fundamental component of the right to life and personal liberty under Article 21, and as part of the freedoms protected by Part III of the Constitution. The Court explicitly overruled earlier pivotal rulings by the Supreme Court in **Kharak Singh vs State of UP AIR 1963 SC 1295 and M.P Sharma vs Satish Chandra**, **AIR 1954 SC 300** which had previously asserted that the Right to Privacy is not a Fundamental Right under the Indian Constitution. [41]

The Constitution of India provides a robust framework for protecting the rights of women against cybercrime. The fundamental rights, directive principles, and judicial interpretations together create a legal environment

[40] AIR (2015) SC 1523
[41] Justice K. S. Puttaswamy (Retd.) and Anr. Vs Union Of India (2017) 10 SCC 1
https://blog.ipleaders.in/justice-k-s-puttaswamy-retd-and-anr-vs-union-of-india/

that demands gender-sensitive laws and effective enforcement. The State, through its legislative and administrative apparatus, is under a constitutional obligation to not only prevent cybercrimes targeting women but also to ensure their access to justice and protection. The constitutional provisions act as both a shield and a sword—shielding women from digital violence and enabling them to seek justice, while obligating the State to adopt proactive and protective legislative measures. The judiciary plays a vital role in this matrix by interpreting these provisions progressively and ensuring they are applied in a manner that truly advances the cause of women's safety in cyberspace. [42]

3.3 : Bharatiya Sakshya Adhiniyam (BSA)

The Bharatiya Sakshya Adhiniyam (BSA) represents a landmark legislative initiative aimed at bolstering India's cybersecurity framework amidst the rapidly evolving digital landscape. Enacted to address the increasing threats posed by cybercrime, terrorism, and data breaches, the BSA establishes a comprehensive set of provisions designed to enhance national security while protecting individual rights. One of its key objectives is to empower law enforcement agencies with enhanced surveillance and investigation capabilities to combat cyber threats effectively. This includes provisions for monitoring online activities and accessing sensitive data when necessary, provided there is due legal process.

The BSA also emphasizes the Importance of data protection, mandating organizations, especially those in critical sectors such as banking and finance, to adopt robust cybersecurity measures to safeguard consumer information. By instituting guidelines for data handling, reporting of data breaches, and establishing accountability mechanisms, the BSA aims to

[42] https://blog.ipleaders.in/everything-about-cybercrimes-against-women/#:~:text=Prior%20to%202013%2C%20there%20was,adding%20Sections%20354A%20to%20354D

create a culture of compliance and vigilance among businesses, fostering greater trust among consumers.

In the digital age, where the proliferation of technology has made data an invaluable asset, the BSA's significance cannot be overstated. It provides a legal framework that aligns with international standards for cybersecurity, ensuring that India can effectively respond to both domestic and global cyber threats. Moreover, the law recognizes the balance between security and privacy, aiming to prevent unauthorized surveillance while addressing legitimate security concerns.

As cyber threats continue to evolve, the BSA's relevance will only grow. Its proactive approach to strengthening cybersecurity infrastructure, combined with its focus on data protection and compliance, positions it as a crucial tool for safeguarding national interests and enhancing individual privacy in an interconnected world. Ultimately, the BSA represents a vital step towards creating a secure digital environment in India. [43]

Section 2(d): Definition of Electronic Evidence

The BSA provides a broad and inclusive definition of "document" to include emails, messages, images, videos, social media posts, chats, digital voice recordings, and metadata. This expanded definition ensures that all forms of digital abuse are recognized and accepted in court. For example, if a woman is harassed via WhatsApp or Facebook, her screenshots, server logs, and digital traces are considered primary evidence under BSA.

Section 61: Admissibility of Electronic Records

Section 61 of the BSA corresponds to the former Section 65B of the Indian Evidence Act and governs the admissibility of electronic records. It maintains the requirement of certificates from responsible officials (such as IT heads or

[43] https://legalonus.com/the-impact-of-bsa-law-on-data-privacy-and-cyber-crimes-in-india-2/

system administrators), verifying authenticity of digital records, date, time, and source of production, device used for data generation.

However, BSA now simplifies procedures, allowing cloud-based and AI-generated data to be admitted with proper authentication—addressing evolving technologies used both in committing and investigating cybercrimes.

Section 62: Presumption of Authenticity

In cases of digital evidence in cyber offences targeting women (e.g., revenge porn, cyberstalking), Section 62 enables the court to presume the authenticity of electronic messages and records unless proven otherwise. This benefits victims by reducing the initial burden of proving the genuineness of content—especially when dealing with offensive emails, harassing DMs, or leaked private videos. This presumption is particularly useful in protecting women from unnecessary cross-examination regarding the origin of the material, thus preserving their dignity.

Section 63: Digital Signature and Identity Authentication

Section 63 emphasizes the importance of digital signatures and identity verification in proving the source of online abuse. In cybercrime cases such as fake profile creation, impersonation using images or names of women, or hacking into private accounts. This provision helps trace and authenticate the originator of the crime through metadata, login credentials, and device footprints. [44]

3.3.1 : Role of BSA in Combating Cyber Crimes:-

The Bharatiya Sakshya Adhiniyam (BSA) law plays a pivotal role in combating cybercrimes by introducing stringent provisions targeting offenses such as hacking, online fraud, identity theft, and data breaches. The BSA seeks to

[44] https://legalonus.com/the-impact-of-bsa-law-on-data-privacy-and-cyber-crimes-in-india-2/

strengthen cybersecurity frameworks by enabling law enforcement agencies to act swiftly against cybercriminals, imposing heavy penalties, and mandating stricter regulations on data protection. These provisions focus on protecting critical infrastructure, financial institutions, and personal data from increasing threats in the digital world. The BSA also emphasizes coordination between various security agencies to improve the detection, investigation, and prosecution of cybercrimes.

A significant strength of the BSA Is its emphasis on punitive measures and its attempt to integrate cybersecurity within the national security discourse. It provides a legal foundation for prosecuting cybercrimes, with provisions addressing digital surveillance, data monitoring, and cooperation with international agencies to tackle cross-border cyber offenses. The law also includes guidelines for businesses and institutions to follow best practices in cybersecurity, making them liable for negligence in data protection. However, potential gaps remain in its enforcement mechanisms. The lack of comprehensive data protection laws and the absence of dedicated cybercrime courts can slow down the prosecution process. Moreover, the law's broad surveillance powers raise concerns about privacy violations, potentially discouraging victims from reporting cybercrimes due to fear of overreach. [45]

A relevant case is **Shreya Singhal v. Union of India (2015),** which struck down Section 66A of the IT Act for violating free speech. This case reflects concerns about government overreach in digital spaces, which is also a risk under the BSA if surveillance and enforcement are not checked. While the BSA provides a robust foundation for combating cybercrimes, stronger privacy protections and specialized enforcement agencies are necessary for effective and ethical implementation.[46]

---

[45] https://legalonus.com/the-impact-of-bsa-law-on-data-privacy-and-cyber-crimes-in-india-2/

[46]. Shreya Singhal v. Union of India, (2015) 5 SCC 1 – The Supreme Court struck down Section 66A of the IT Act for violating free speech, underscoring the need to balance enforcement with privacy and civil liberties under laws like the BSA.

The Bharatiya Sakshya Adhiniyam (BSA) marks a significant advancement In India's legislative framework for addressing the complex challenges posed by cybercrime and data privacy in an increasingly digital world. By integrating national security concerns with stringent provisions for data protection, the BSA aims to create a robust mechanism to combat cyber threats while safeguarding individual rights. However, as the digital landscape evolves with advancements in technology such as artificial intelligence and block-chain, it is crucial for the BSA to adapt and enhance its provisions to effectively address emerging cyber risks and privacy challenges.

The law's Implementation has spurred businesses and financial institutions to adopt more rigorous data security practices, fostering a culture of compliance that prioritizes consumer protection. Nevertheless, the potential for overreach in surveillance powers necessitates a careful balance between national security interests and individual privacy rights. Legal safeguards must be established to ensure that the power to monitor and access personal data is exercised judiciously and transparently, with adequate oversight mechanisms in place.

Future reforms should focus on clarifying the legal definitions of cybercrimes, enhancing privacy protections, and incorporating ethical considerations in the use of technology. By doing so, the BSA can evolve into a comprehensive framework that not only mitigates cyber threats but also upholds the fundamental rights of individuals.

Ultimately, the successful implementation of the BSA requires a collaborative effort among lawmakers, law enforcement, businesses, and civil society to create an environment where data privacy is respected, and cybersecurity is prioritized, ensuring a safer digital future for all citizens in India.[47]

[47] https://legalonus.com/the-impact-of-bsa-law-on-data-privacy-and-cyber-crimes-in-india-2/

3.4 : Indian Penal Code, 1860

Before 2013, there was no specific legislation addressing online harassment or crimes against women in cyberspace. **Section 354A** of the 2013 Criminal Amendment Act modifies the Indian Penal Code, 1860 by introducing **Sections 354A** to **354D**.

Section 354A stipulates that if a man engages in any of the following actions — requesting or soliciting sexual services; displaying pornography without a woman's consent; or making sexual comments — it constitutes sexual harassment and may result in severe imprisonment for up to 3 years, or a fine, or both. In the cases of the first two actions, the punishment can include up to one year of imprisonment, a fine, or both.

Section 354C defines 'voyeurism' as the act of capturing and/or disseminating an image of a woman engaged in a private act without her consent. To be classified as 'Voyeurism,' the circumstances must be such that the woman would "reasonably expect not to be seen, either by the offender or by anyone acting under the perpetrator's authority." A person found guilty under this section faces a fine and a maximum of three years' imprisonment for a first offense, and up to seven years for subsequent offenses.

Section 354D imposes a prohibition on stalking that extends to online stalking. Stalking is described as an action where a man pursues or contacts a woman despite her clear lack of interest, or monitors a woman's online activities or use of electronic communication. A man convicted of stalking may face up to three years in prison and a fine for a first offense, and up to five years in prison and a fine for subsequent convictions. [48]

[48] https://blog.ipleaders.in/everything-about-cybercrimes-against-women/#:~:text=Prior%20to%202013%2C%20there%20was,adding%20Sections%20354A%20to%20354D
https://blog.ipleaders.in/punishments-cyber-crimes-ipc/#Cyber_crimes_with_IPC_implications

In the case of **Kalandi Charan Lenka v. The State of Odisha, 2017** the victim received certain inappropriate messages from an unknown number that harmed her reputation. Additionally, emails were sent, and a fake Facebook account was created by the accused, which featured manipulated images of the victim. Consequently, the accused was found prima facie guilty of cyberstalking by the High Court under various provisions of the IT Act and **Section 354D** of the IPC. [49]

Section 465 of the IPC: In the context of cyber activities, crimes such as email spoofing or the creation of fake documents are governed by this provision, which can result in imprisonment of up to 2 years, a fine, or both. In the case of **Anil Kumar Srivastava** v. **Addi Director**, **MHFW (2005),** the petitioner electronically forged the signature of the AD and subsequently filed a complaint with false accusations against this individual. The court determined that the petitioner was liable under Section 465 as well as Section 471 of the IPC due to the use of the forged signature as a valid document.[50]

Section 500 of the IPC: This section penalizes the defamation of any individual. In the context of cybercrimes, sending any defamatory content or abusive communications via email falls under Section 500 of the IPC. The imprisonment duration under this section can be up to two years along with a fine.

Section 506 of the IPC: If someone attempts to intimidate another person criminally, either physically or electronically, concerning their life, the destruction of property by fire, or a woman's chastity, this is regarded as an offense under Section 506 of the IPC, which carries a potential maximum imprisonment of seven years or a fine, or both. [51]

---

[49]Kalandi Charan Lenka v. The State of Odisha, 2017, SCC OnLine Ori 36

[50]Anil Kumar Srivastava v. Addi Director, MHFW (2005), SCC OnLline All, 1384.

[51] https://blog.ipleaders.in/punishments-cyber-crimes-ipc/#Cyber_crimes_with_IPC_implications

3.5 : Bhartiya Nyaya Sanhita (2023)

With the repeal of the Indian Penal Code, 1860, and the enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS), India has taken a significant step toward modernizing its criminal laws to address emerging challenges, including cybercrimes against women. This reform reflects the changing socio-technological landscape, recognizing the unique and increasing threats faced by women in the digital age. Cyberstalking, online sexual harassment, impersonation, and distribution of non-consensual images have become more frequent, and BNS attempts to provide clearer, more gender-sensitive provisions to deal with such offences. [52]

Several provisions in the BNS address offences that occur via electronic communication, thus explicitly acknowledging the cyber dimension of crimes that were earlier prosecuted under broader terms in the IPC.

Section 69 – Assault or Criminal Force to Woman with Intent to Outrage Her Modesty (formerly IPC Section 354)

This section retains the essence of the IPC but is expanded to include digital forms of assault or harassment that affect the modesty of a woman. Online behaviour such as sending obscene messages, sexual threats, or unwelcome advances through email or social media can fall under this provision if they are intended to outrage modesty.

Section 70 – Sexual Harassment (Expanded from IPC Section 354A)

The BNS includes explicit reference to electronic communication as a means of committing sexual harassment. It covers sending sexually colored remarks, demanding or requesting sexual favors through messages or calls, showing pornography through digital means, making unwelcome physical or virtual

[52] https://www.drishtijudiciary.com/to-the-point/bharatiya-nyaya-sanhita-C-indian-penal-code/organised-crime

advances. This inclusion helps to criminalize cyber sexual harassment, which has become rampant on social media and dating platforms.

Section 71 – Assault or Use of Criminal Force with Intent to Disrobe a Woman (formerly IPC Section 354B)

This section is relevant in cases where digital content such as manipulated or morphed images is used to portray a woman in a state of undress or humiliation. Though primarily meant for physical acts, its interpretation can be extended to cyber offences involving coerced video calls or the misuse of intimate images to publicly shame women.

Section 74 – Voyeurism (Earlier IPC Section 354C)

Voyeurism, including capturing images or videos of a woman engaged in a private act without consent, is now clearly penalized under BNS. This also includes cyber voyeurism, where such content is captured via hacked webcams, or shared over messaging platforms. The repeated viewing or dissemination of such content online also falls under this section, strengthening the law against revenge porn and non-consensual pornography.

Section 75 – Stalking (including Cyberstalking)

Stalking under BNS includes following a woman physically or through electronic communication, monitoring her online activity, or sending repeated messages despite resistance. This section is critical for addressing cyberstalking on social media, email harassment, persistent messaging or surveillance through tracking apps. This broader definition recognizes the psychological trauma caused by digital surveillance and intrusion. [53]

[53] https://www.drishtijudiciary.com/to-the-point/bharatiya-nyaya-sanhita-C-indian-penal-code/organised-crime

The interpretation and implementation of these provisions should align with judicial directives mandating sensitive handling of women victims, especially in cybercrime cases. Investigating officers are expected to respect a woman's dignity and privacy while recording statements, which should preferably be done by female officers.

BNS provisions impose stricter punishments for repeat offenders. In cybercrime cases, where harassment often escalates over time, this acts as a significant deterrent. Although BNS is a newly enacted legislation, its continuity with IPC allows for the continued application of precedents and judicial interpretations laid down under the IPC.[54]

3.6 : Bharatiya Nagarik Suraksha Sanhita, (2023)

The enactment of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 represents a crucial step forward in reforming India's criminal justice system, particularly in addressing the complexities of modern-day crimes such as cybercrimes targeting women. With the digital transformation of society, new forms of violence and harassment have emerged, and the legal framework had to evolve to meet these challenges. BNSS addresses several aspects of cybercrime, especially those that disproportionately affect women, including cyberstalking, online harassment, non-consensual pornography, and identity theft.[55]

With the increasing use of social media, messaging platforms, and digital communication, women are exposed to new forms of harm. The BNSS, 2023 is a comprehensive effort to address these issues by defining and punishing

[54]The BNS emphasizes victim-sensitive procedures, including statement recording by female officers, and introduces enhanced penalties for repeat offenders—key in cybercrime cases involving escalating harassment. Though new, it retains continuity with the IPC, allowing prior judicial interpretations to remain relevant.

[55] The BNSS, 2023 modernizes procedural law to address emerging crimes, including cyber offences disproportionately impacting women, such as cyberstalking, online harassment, and non-consensual pornography, reflecting the need for a responsive legal framework in the digital age.

these offences while offering mechanisms for protection, redressal, and victim compensation.

Cyberstalking and online harassment have become major concerns for women in the digital era. Under BNSS **Section 72**, cyberstalking includes persistent online monitoring, harassing messages, or threats over digital platforms like social media, email, or instant messaging services.

Cyberstalking is defined as using electronic communications to follow, monitor, or threaten a woman, often leading to severe mental and emotional distress. This section expands the scope of harassment by recognizing electronic stalking, which includes monitoring or tracking someone's online activities without consent. BNSS addresses the growing prevalence of digital harassment by criminalizing acts that were previously not explicitly punishable under earlier laws.

This provision of BNSS focuses on voyeurism, traditionally understood as secretly observing a person's intimate acts. With the advent of technology, digital voyeurism has emerged as a prevalent form of abuse. BNSS under **Section 74** specifically criminalizes the unauthorized recording, sharing, or distribution of intimate images, use of hidden cameras or surveillance equipment to capture private moments, non-consensual creation or circulation of sexual content involving women. [56]

The law recognizes the potential for revenge porn and non-consensual pornography as forms of cybercrimes and makes it a criminal act to share or distribute such material without the woman's consent. This provision is particularly relevant given the rising number of cases involving image-based sexual abuse.

[56] https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nagarik_Suraksha_Sanhita,_2023.pdf

Section 80 – Non-Consensual Sharing of Intimate Images

The non-consensual sharing of intimate images is a growing issue, often related to the phenomenon of revenge porn. Section 80 of BNSS specifically criminalizes the sharing of intimate or explicit images without consent. This includes both the act of creating and distributing such images.

Women who are victims of revenge porn, where intimate images or videos are shared as an act of vengeance, can now seek legal protection and remedy under this provision. This provision recognizes the emotional and psychological toll such acts have on victims and ensures that they are not left without recourse.

BNSS includes provisions aimed at victim protection, ensuring that women who are victims of cybercrimes receive appropriate support. This includes protection orders to prevent further online harassment, access to legal aid, and psychological support for victims dealing with trauma due to cybercrimes. The law empowers the judiciary to provide relief quickly and to ensure that the rights of the victim are prioritized during the judicial process.

BNSS also calls for the establishment of specialized courts or cybercrime tribunals dedicated to hearing cases related to cybercrimes against women. These courts would have trained personnel, including judges and technical experts, to handle such sensitive and technically complex cases efficiently. [57]

[57] https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nagarik_Suraksha_Sanhita,_2023.pdf

3.7 : The Information Technology Act of 2000 and its amendments

The Information Technology Act of 2000 (ITA) marks a pivotal moment in India's commitment to recognizing online commercial transactions, also referred to as Electronic commerce (e-commerce). This was enacted to align with the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL).

Notably, the primary intent of the ITA was to facilitate e-commerce, rather than focus on cyber crimes. The ITA included some provisions that deemed activities such as hacking and digital obscenity as punishable offences, yet it did not establish a comprehensive law addressing cyber crimes broadly. It was only in 2009 that the Information Technology Amendment Act of 2008 (ITAA) introduced more extensive amendments to the ITA, defining and punishing various cyber crimes. As computer and internet use surged in everyday life, so did criminal activities, highlighting the inadequacies of the ITA in addressing cyber crimes effectively. Between 2000 and 2009, relevant sections of the IPC were utilized to prosecute cyber offenders. Interestingly, the first conviction in India for stalking in cyberspace was achieved under Section 354 of the IPC (which punishes outraging the modesty of a woman).

India has made significant strides in addressing cybercrime through various laws, but there are still gaps, especially regarding crimes against women. The Information Technology (IT) Act of 2000 serves as India's primary regulatory framework for cyber activities and for combatting various forms of cyber crime, particularly those targeting women. Initially enacted to promote e-commerce, data protection, and privacy, its application has gradually expanded to encompass prevention of cyber crimes. [58]

---

[58] General Assembly of United Nations, resolution no. A/RES/51/162 (30 January,1997).
Chapter XI of the ITA in Ss. 65, 66, 67, 71, 72, 73 and 74 defined certain acts as punishable. However, this Chapter did not provide for a comprehensive general law on cyber crime.
Act 10 of 2009 (w.e.f. 17/10/2009).

Section 66E (Violation of Privacy): This section punishes the unauthorized capture, publication, or transfer of photographs depicting a person's private areas. It aims to safeguard privacy, especially that of women, by penalizing the unauthorized dissemination of intimate images. Offenders may face up to three years in prison, a fine of two lakh rupees, or both. Section 67 (Punishment for Publishing or Transmitting Obscene Material in Electronic Form): This section criminalizes the electronic dissemination and transmission of obscene materials, including pornography. The penalty for a first offence can be up to three years of imprisonment and a fine of five lakh rupees. Subsequent violations can lead to incarceration for up to five years, along with a fine reaching ten lakh rupees.

Section 67A (Punishment for Publishing or Transmitting Sexually Explicit Material): Section 67A addresses the publication or transmission of sexually explicit content, imposing stricter penalties compared to Section 67. A first-time offender could face up to five years in prison and a fine up to ten lakh rupees, while repeat offenders may be punished with imprisonment spanning up to seven years. **Section 67B** (Punishment for Child Pornography): This section makes it illegal to publish or transmit materials that show minors engaged in sexually explicit acts. The punishment mirrors that of Section 67A, but holds particular significance in cases involving the exploitation of children online. [59]

Section 67-F of the ITA establishes penalties for cyber terrorism and also offers a definition for it. The definition of cyber terrorism is broad enough to encompass unauthorized entry or access to computer resources, information, data, or databases that are restricted for reasons related to national security or foreign relations. Additionally, Section 15 of the Unlawful Activities Prevention Act, 1967 categorizes it as a "terrorist act." Therefore, engaging in

---

[59] Pawan Duggal, "India's First Cyber Stalking Case- Some Cyber Law Perspectives", available at http://cyberlaws.net/cyberindia/2CYBER27.htm (accessed on 14/06/2016)
Kaul, V., C Sinha, M. (2020). "Cyber Crimes in India: Legislative and Judicial Response."

any of these activities using a computer or computer network will be classified as cyber terrorism. [60]

Previously, cyber stalking and cyber bullying were addressed under Section 66A of the ITA, but in the case of **Shreya Singhal** v. **Union of India**, **(2015) 5 SCC 1** the Supreme Court ruled this provision unconstitutional as it violated Articles 19 and 21 of the Constitution. The Supreme Court held that Section 66A was vaguely worded and directly impacted the public's right to know. By creating offenses against individuals who use the internet to annoy or inconvenience others, this section clearly infringed on the freedom of speech and expression of the citizens of India as a whole. Consequently, Section 66A disproportionately and arbitrarily violates the right to free speech and disturbs the balance between that right and any reasonable restrictions that could be applied, rendering it unconstitutional due to its inclusion of protected speech and innocuous statements. [61]

In the absence of Section 66A, cyber stalking and cyber bullying can be prosecuted under Sections 66-E and 67-A of the ITA. Furthermore, Section 354 of the Code provides penalties for the cyber stalking of women. Other sections of the Code, including 292, 292-A, 293, 294, 469, 500, 507, and 509, may also be relevant in cases of cyber stalking.

The case of **Suhas Katti** v. **State of Tamil Nadu** in **(2004)** was the first instance in India involving the controversial provision of the IT Act, 2000, specifically Section 67 related to the publication or transmission of obscene material. In this case, the accused, who was a friend of the victim and had feelings for her, faced rejection from her. Later, after the victim got married and subsequently decided to divorce, Suhas, wishing to rekindle contact, was rejected again. Angered, Suhas chose to take revenge by harassing her online, sending emails under her name to random individuals, which led many to

[60] Verma, A. 2021." The rising Tide of Cyberstalking and Harassment in India: A Gendered Perspective
[61]Shreya Singhal v Union of India, AIR, 2015, 5 SCC 1
http://csciwww.etsu.edu/gotterbarn/stdntppr/cases.htm (last accessed on 26/07/2016).

believe that she was soliciting clients as a prostitute. Ultimately, the victim filed a complaint, resulting in Suhas being charged under Sections 469, 509 of the IPC and Section 67 of the IT Act. He was sentenced to two years of rigorous imprisonment under Section 469 IPC, one year of simple imprisonment under Section 509 IPC, and two years of imprisonment under Section 67 of the IT Act, so five years, along with a fine of Rs 5000.

The IT Act, 2000 takes precedence over the provisions of the IPC concerning cybercrimes, although there are many instances where IPC provisions are applied depending on the specific details of each case. Some argue that the IPC should not govern cybercrimes, yet there are several cyber offenses that the IT Act, 2000 does not adequately address. Therefore, once the necessary amendments are made to the IT Act concerning all cybercrimes, the IPC may be withdrawn from regulating the area of cybercrime. [62]

3.8 : Other Legislation Safeguarding Women in the Digital Realm

3.8.1 : Digital Personal Data Protection Act (2023)

Before the passing of the DPDPA, 2023 in India there were various other acts, rules, bills, cases, and drafts that dealt with the privacy of the personal data of individuals.

The first law that was enacted to secure the digital information of individuals was Information Technology Act, 2000. Later in the year 2011, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 came into force to secure the sensitive personal data or information of individuals.[63]

---

[62] https://blog.ipleaders.in/laws-pertaining-to-online-harassment-of-women/#Suhas_Katti_v_State_of_Tamil_Nadu_2004
https://blog.ipleaders.in/pocso-act-everything-you-need-to-know/#Introduction

[63] Before the DPDPA, 2023, India addressed data privacy through laws like the IT Act, 2000 and the IT Rules, 2011, which were early efforts to regulate digital information and protect sensitive personal data.

Further, the Ministry of Electronic and Information Technology codified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to balance the privacy rights in the interest of national security and public order. [64]

In the case of **Karmanya Singh Sareen and Anr vs. Union of India and Ors. (2016)**, WhatsApp's 2016 privacy policy to permit WhatsApp to share data with Facebook was challenged before the Delhi High Court, wherein the High Court upheld WhatsApp's policy and directed them to delete the data of the users who have opted out from this service. [65]

In the case of **Justice K S Puttaswamy (Retd.), and Anr. Vs. Union of India,(2012),** the 9 judges' bench of the Supreme Court of India declared that the right to privacy is a fundamental right of the person under Article 21 of the Constitution of India. Following this, the B.N. Shrikrishna committee was formed to report on the concerns regarding the digitalization of personal data and propose solutions. The Draft Personal Data Protection Bill, 2018 was drafted by the committee which was presented before the lower house of the Parliament. Later in the year 2019, the draft Bill of 2018 was referred to the joint parliamentary committee for examination and was for public comments.[66]

Now, after 5 years of extensive submissions, discussions, recommendations, consultations, customizations, and deliberation, a final draft of the Digital

[64] The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were introduced by the Ministry of Electronics and IT to regulate digital platforms, aiming to balance user privacy with national security and public order concerns.

[65] . Karmanya Singh Sareen C Anr. V. Union of India C Ors., (2016) – The Delhi High Court upheld WhatsApp's 2016 privacy policy but directed deletion of user data for those who opted out, highlighting concerns over data sharing and user consent.

[66] Justice K.S. Puttaswamy (Retd.) C Anr. V. Union of India, (2017) 10 SCC 1 – The Supreme Court recognized the right to privacy as a fundamental right under Article 21. This led to the formation of the B.N. Srikrishna Committee, which drafted the Personal Data Protection Bill, 2018, later revised and referred to a Joint Parliamentary Committee in 2019.

Personal Data Protection Bill, 2023, which after approval from the cabinet, was finally ready to be presented before the houses of the parliament and finally got passed in the lower house.[67]

Objectives of the Act [68]

The objectives of the DPDP Act are:

• to govern the processing of personal data on the digital platform in India whether obtained online or offline;

• to provide for the protection of digital personal data;

• to lay down grounds for processing personal data;

• to make provisions that will harmonise the ever-evolving digital infrastructure and technological advancement in India with the core fundamental right of privacy of its individuals;

• to place general and in certain cases special obligations on entities that process personal data;

• to confer rights in respect of their personal data on individuals;

• to provide for the duties of the individual while exercising their rights and providing their personal data for certain purposes;

• To lay down a digital design compliance framework for easy and faster implementation of the proposed Act;

• to regulate digital technology by ascertaining the accountability of Al-driven applications and platforms while handling personal digital data;

[67] After five years of deliberation and stakeholder input, the Digital Personal Data Protection Bill, 2023 was finalized, approved by the Cabinet, and subsequently passed in the Lok Sabha, marking a significant step in India's data protection regime.

[68] https://legalonus.com/the-impact-of-bsa-law-on-data-privacy-and-cyber-crimes-in-india-2/

• to enable parties in dispute to attempt for mediation;

• to provide for monetary penalties for noncompliance of the provisions of the Act; and

• to enable voluntary undertaking for faster resolution and rectification of lapses.

The Indian Digital Personal Data Protection Act, 2023 is a unique combination and compilation of the currently existing legislations on data protection around the world. India has learned and taken guidance from data protection regimes like the USA, China, Australia, etc.

Though the basic structure of the Act is taken from General Data Protection Regulation, there are some key differences in the Act like wide powers to the Central Government, limited ground for processing, no right to data portability, no strict requirements for data localization, and no provision for special categories of personal data. Through this Act, the legislature has aimed to safeguard the personal data of the individual and has addressed the privacy of individuals and cross-border transfer of personal data. The drafting of this Act is intended to strike a balance between Indian law relating to data privacy and foreign laws on international trade, especially data-driven businesses.

However, the Act still is required to be more refined and detailed in certain aspects which are discussed above and we can expect the evolution of this law according to the changing scenarios of the society through amendments undertaken in future. [69]

[69] https://legalonus.com/the-impact-of-bsa-law-on-data-privacy-and-cyber-crimes-in-india-2/

3.8.2 : Indecent Representation of Women (Prohibition) Act, 1986

The Indecent Representation of Women (Prohibition) Act, 1986, was established to control how women are depicted in mainstream media, especially in print media. This law forbids indecent representation through several mediums, including publications, advertisements, paintings, images, and brochures. Its goal is to assure that women are not portrayed in an "indecent" manner in the media. The Act, which is still applicable today, primarily addresses print media and advertising.

While the Indecent Representation of Women (Prohibition) Act, 1986 (IRWA) stands as a pivotal measure in confronting the depiction of women in traditional media, it does not adequately address the issues presented by the digital era. With the rise of social media and advancements in artificial intelligence, there is a pressing necessity for legislative changes to address modern forms of communication and expression. The existing provisions in Sections 3 and 4 of IRWA, along with relevant segments of the Indian Penal Code (IPC) and the Information Technology Act, 2000, lay down a foundation for tackling indecent representation. However, they do not expressly encompass the swiftly changing digital realm, including social media platforms, AI-generated content, and other electronic means of communication.[70]

Important legal precedents, such as **Ranjith D. Udeshi** v. **State of Maharashtra (1965)** and **Aveek Sarkar** v. **State of West Bengal**,**(2014)**[71] illustrate the judiciary's changing perspective on obscenity and indecent representation. The shift from the Hicklin Test to the community standards test signifies a more progressive viewpoint; however, applying these tests to digital content is still not well-developed. The proposal of the Indecent

[70] https://blog.ipleaders.in/the-indecent-representation-of-women-prohibition-act-1986-in-time-of-social-media/

[71] Ranjith D. Udeshi v. State of Maharashtra (1965) SC 881
State of Maharashtra (1965) and Aveek Sarkar v. State of West Bengal, (2014) 4, SCC 257

Representation of Women (Prohibition) Amendment Bill, 2012, represented a positive development, intending to fill these gaps by adding definitions for "electronic form" and broadening the definition of "publish." Nevertheless, its retraction in 2021 signifies a lost opportunity to update the legal framework. It is essential for legislators to revisit and revise the IRWA, as well as the pertinent sections of the IPC and the IT Act, to specifically include and address the challenges presented by social media and AI-generated content. Such revisions should focus on establishing clear definitions and effective measures to protect women's dignity in the digital age, ensuring that legal safeguards keep pace with technological progress. This strategy will better prepare the legal system to maintain public morality and shield individuals from indecent representation across various media formats.

With technological advancements, troubling aspects of the dark web are emerging that are concerning. The Internet has turned into a means for malicious acts that are exploited by cunning individuals for immoral purposes and sometimes for financial advantage. Therefore, at this juncture, cyber laws become relevant and hold significance for all citizens. Given that cyberspace is a highly complex realm to navigate, certain activities are deemed grey areas that existing laws may not regulate. [72]

Therefore, in the Supreme Court case of **Sampurna Behura vs. Union of India (2018),**[73] an order was issued on August 2, 2018, prohibiting electronic media from publishing or broadcasting images of minor girls, even if altered or obscured. While the POCSO Act stands as a distinct, comprehensive law addressing offenses against children, it should not be interpreted as a complete legal framework. Several other laws, such as the Bhartiya Nagarik Suraksha Sanhita, 2023 (previously the Code of Criminal Procedure, 1973), the Bhartiya Nyaya Sanhita, 2023 (formerly IPC, 1860), the Juvenile Justice Act, 2015, and the Information Technology Act, 2000, often intersect with or

[72] https://blog.ipleaders.in/the-indecent-representation-of-women-prohibition-act-1986-in-time-of-social-media/

[73] Sampurna Behura vs. Union of India (2018), 4 SCC 433

complement the POCSO Act's provisions. Nevertheless, if there is a conflict between the POCSO Act and any other legislation, Section 42-A of the POCSO Act stipulates that its provisions will take precedence.

3.9 : Summary

In India and around the world, as people increasingly depend on technology, the need for cyber laws to be continually updated and refined is crucial. The rise in remote work due to the pandemic has also heightened the demand for application security. Lawmakers must exercise added caution to stay ahead of fraudsters so that appropriate action can be taken as issues arise. This can be mitigated if legislators, internet providers, banks, shopping websites, and other intermediaries collaborate. Ultimately, however, it is the responsibility of users to engage in the fight against cybercrime. The advancement of online safety and resilience can only occur by considering the efforts of these stakeholders and ensuring they act within the boundaries of cyberspace law. [74]

This chapter examines the legislative provisions in India aimed at combating cybercrimes against women. It discusses the relevance of constitutional protections—such as the right to equality, non-discrimination, freedom of expression, and the right to privacy—as foundational guarantees. The chapter reviews key provisions of the Information Technology Act, 2000 and the Indian Penal Code, 1860, which criminalize acts like online stalking, harassment, and the circulation of obscene material. Recent criminal law reforms including the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA) are also examined for their victim-centric orientation and modern approach to digital evidence.

[74] https://blog.ipleaders.in/the-indecent-representation-of-women-prohibition-act-1986-in-time-of-social-media/

Chapter-4

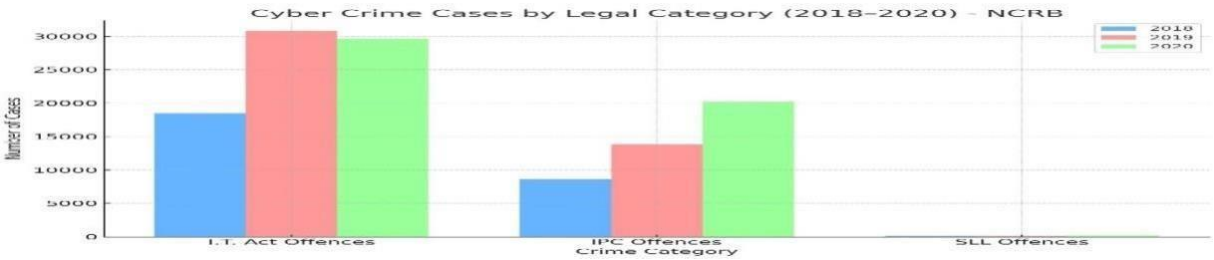
Role Of Judiciary In Protecting Victims Of Cyber Crime

Judicial interpretation of laws related to cybercrime affecting women victims

4.1 : Introduction

The judiciary has played a crucial role in addressing crimes perpetrated in cyberspace through its proactive engagement and intervention. It has consistently made essential interventions to protect the rights and freedoms of individuals in society, particularly focusing on women and children, who represent vulnerable groups.

The rise of the digital era has led to the increase of cybercrime, which threatens various aspects of our lives. The growing incidence of cybercrime targeting women and children in India has become a notable concern in recent times. The advancement of technology and the internet has equipped offenders with new avenues to exploit, harass, and victimize at-risk individuals. In this context, the role of the judiciary in addressing cybercrime against women and children is critically important. The judiciary plays a vital role in interpreting and enforcing legal statutes, ensuring fairness, and safeguarding the interests and well-being of individuals.[75]



[75] Sanyogita and Singh, "Role of Judiciary in Curbing Cybercrimes", Commonwealth L. Rev. J., Vol. 9 (2023). Source : National Crime Records Bureau (NCRB), Crime in India Report, Ministry of Home Affairs, Government of India, 2018-2020 Available at: https://ncrb.gov.in

Case Laws

4.2 : Mrs. X v. Union of India and Others (2023)[76]

The case of Mrs. X v. Union of India and Others (2023) involves the cybercrime known as Non-consensual dissemination of intimate images also commonly referred to as “revenge porn”.

Facts of the Case:

In the case of Mrs. X v. Union of India and Others, the Supreme Court of India was confronted with a deeply disturbing issue involving cybercrime and the violation of an individual’s privacy and dignity. The petitioner, anonymized as “Mrs. X” to protect her identity, approached the Court after her intimate and sexually explicit images and videos were unlawfully disseminated online without her knowledge or consent. These materials were published on several pornographic websites and circulated through messaging platforms like WhatsApp and Telegram.

Despite lodging multiple complaints with cybercrime cells, local police authorities, and internet intermediaries such as Google, Meta (Facebook, Instagram), and the administrators of the websites involved, there was inordinate delay and inaction in removing the content. The petitioner claimed severe emotional trauma, loss of reputation, social isolation, and fear for personal safety. She contended that the failure of both State and private actors to protect her from ongoing digital victimization constituted a gross violation of her fundamental rights under Article 21 of the Constitution, which guarantees the right to life and personal liberty, including the right to privacy and dignity.

[76] Mrs. X v. Union of India C Ors., 2023 SCC OnLine SC 818. This Is a landmark Supreme Court case where the Court emphasized the protection of a sexual assault survivor’s identity and privacy after her video was unlawfully circulated online.

Types of Evidence Used

A wide range of digital and documentary evidence was submitted before the Court to substantiate the petitioner's claims:

1. Digital Evidence: Screenshots of the explicit content from various platforms, URLs and hyperlinks of the webpages hosting the material, Chat logs from messaging platforms showing the circulation of these materials.
2. Cyber Forensic Reports: Government-certified cyber forensic experts examined the digital evidence and confirmed the authenticity of the images and videos, as well as the timeline of their uploads and digital footprints. IP address tracing reports were submitted to identify the potential origin of uploads.
3. Official Records of Complaints: Copies of the FIRs, email correspondences, and RTI replies reflecting administrative delays. Notices and responses (or lack thereof) from intermediaries under the IT Act, 2000.
4. Expert Affidavits and Legal Submissions: Affidavits from legal and technology experts explaining the obligation of intermediaries under Rule 3 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Grounds for accepting and rejecting evidence

Accepted Evidence:

Forensically authenticated digital content, including screenshots and URLs with verifiable metadata.

Cyber forensic reports were accepted as credible and authoritative, given that they were issued by government-recognized labs.

Official complaint records and intermediary responses were admitted to establish the timeline and response failure.

Rejected Evidence:

Some unverified social media links and anonymous third-party content were excluded due to the inability to trace origins or authenticate the source.

Screenshots lacking metadata, timestamps, or forensic backup were considered insufficient as standalone proof.

Judgment

The Supreme Court ruled in favor of the petitioner, delivering a robust judgment that reasserted the role of the judiciary in upholding digital rights and protecting victims of cybercrime. The Court emphasized that non-consensual publication of intimate content online constituted a serious form of cyber sexual harassment, and the inaction of the authorities violated her right to privacy, dignity, and protection from mental cruelty.

The Court directed immediate takedown of all offensive content by intermediaries and internet service providers; mandating that the Union Government establish a fast-track grievance redressal mechanism, with a mandatory response time of 72 hours for content takedown in cases involving sexual harassment; issuing guidelines for proactive monitoring and due diligence by intermediaries under the IT Rules, 2021, making them accountable for not acting on complaints swiftly; monetary compensation to Mrs. X for the emotional trauma, reputational damage, and prolonged victimization she suffered. The Court also highlighted the need for capacity building within the police and judiciary for handling cybercrime against women more sensitively and efficiently.

This case is a landmark in the development of victim-centric jurisprudence in cyber law. It showcases how the judiciary has stepped in to bridge legislative and enforcement gaps, particularly when statutory mechanisms have failed to provide timely redress to victims. The judgment reflects judicial activism, interpreting fundamental rights expansively to include protection against

Mrs. X v. Union of India C Ors., 2023 SCC OnLine SC 818

digital harm, and sets precedent for holding both public authorities and private intermediaries accountable.

By ensuring prompt takedown of offensive material, holding intermediaries responsible, and ordering compensation, the Court in Mrs. X demonstrated how the judiciary can act as a guardian of victims' rights in cyberspace and strengthen the legal framework against online violence targeting women.

4.3 : Ritesh Sinha v. State of Uttar Pradesh (2019)[77]

The case Ritesh Sinha v. State of Uttar Pradesh (2019) involves the cybercrime of impersonation and fraud using telecommunication devices.

Facts of the case:

The case of Ritesh Sinha v. State of Uttar Pradesh dealt with a significant issue relating to the collection of electronic evidence in criminal investigations and the rights of the accused under Article 20(3) of the Constitution, which protects individuals from self-incrimination.

The petitioner, Ritesh Sinha, was accused of impersonating a police officer and making fraudulent phone calls to extract information and money. During the investigation, the prosecution believed that Ritesh had used a specific mobile phone number to commit the offense. The investigating agency sought to record his voice sample to compare it with the recorded conversations found on the victim's phone. However, Ritesh refused to voluntarily provide his voice sample.

The prosecution moved an application before the Magistrate to compel Ritesh to give his voice sample. The Magistrate directed him to comply, but Ritesh challenged this order, arguing that there was no statutory provision that empowered the Magistrate to issue such a direction. The case eventually reached the Supreme Court, raising important questions about the legality of

[77] Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1. This Supreme Court judgment dealt with the legal validity of compelling an accused to provide voice samples during a criminal investigation—an important precedent for digital and cyber forensic evidence in criminal law.

collecting voice samples and its implications on personal liberty and protection against self-incrimination.

Types of Evidence Used:

The primary evidence involved in this case was electronic and biometric in nature:

1. Voice Recordings: The prosecution relied on audio recordings of the phone calls made to the victim. These recordings were the central piece of evidence.
2. Call Detail Records (CDRs): These records were used to establish that the calls originated from a particular mobile number linked to the accused.
3. Proposed Voice Sample: The investigating agency sought to compare Ritesh's voice sample with the recorded voice to confirm his involvement.
4. Mobile Forensic Analysis: A forensic expert's report was anticipated to examine the match between the sample voice and the recorded calls.

This case is especially important in the context of cyber crime because voice calls made using mobile phones and internet-based applications like VoIP (Voice over Internet Protocol) are now common tools in committing cyber frauds, impersonation, and online threats.

Grounds for Accepting and Rejecting Evidence:

Accepted:

The recorded phone conversations were accepted as valid evidence under the Indian Evidence Act, provided that they were authenticated and had proper certification under Section 65B.

The CDRs and mobile location data were treated as circumstantial evidence connecting the accused to the crime scene and device used.

The Court acknowledged the importance of biometric and forensic evidence, such as voice samples, in the modern digital crime landscape.

Contested (and initially rejected):

The main legal issue was whether the Magistrate had the power to compel a person to provide a voice sample in the absence of specific statutory authority.

The defense argued that this act would violate the accused's right against self-incrimination under Article 20(3) of the Constitution, as voice is a personal and identifying characteristic.

Earlier judgments had left this issue unresolved due to the lack of clarity in the Code of Criminal Procedure (CrPC) regarding voice samples.

Judgment

The Supreme Court, in a 3-judge Bench decision authored by Justice Deepak Gupta, held that in the interest of justice and effective investigation, the Magistrate does have the implied power to direct an accused to provide a voice sample, even in the absence of explicit statutory authority under the CrPC.

The Court observed that with the advancement of technology and the increasing complexity of cyber and digital crimes, traditional methods of investigation are often insufficient. It emphasized that voice samples are not testimonial in nature but are similar to fingerprints, handwriting, or DNA—used to establish identity, not to compel self-incriminating speech.

The Court balanced this reasoning with safeguards, stating that such directions must be made only by a Judicial Magistrate after proper application of mind, and only when it is necessary for the purposes of investigation.

Moreover, the Court urged the legislature to amend the law to provide a clear statutory basis for collecting voice samples, acknowledging that reliance on implied powers should be temporary and exceptional. This judgment has far-reaching implications in cyber crime cases, especially those involving impersonation and fraud over calls or digital platforms, cyberstalking or threatening voice messages, and online financial scams using voice assistants or VoIP calls. In such cases, voice samples may be the only way to identify and prosecute the offender. By allowing courts to compel voice samples, the judiciary played a critical role in strengthening investigative capabilities and

ensuring that victims of cybercrime are not left helpless due to technical limitations in evidence collection.

The ruling in Ritesh Sinha thus represents a proactive judicial approach to adapting criminal procedure to meet the challenges of digital evidence and online crimes. It upholds the balance between constitutional rights and the need for effective law enforcement, especially when dealing with the increasing threat of cyber offences.

4.4 : State of Kerala v. Rahul Pasupalan and Another (2019)[78]

Facts of the Case:

In 2015, the Kerala Crime Branch initiated "Operation Big Daddy" to dismantle an online sex trafficking network operating within the state. This investigation led to the arrest of social activists and former "Kiss of Love" campaigners, Rahul Pasupalan and his wife, Resmi R. Nair. The couple was accused of orchestrating an online prostitution ring that exploited women and minor girls, some trafficked from Bengaluru to Kerala.

The operation was triggered by a Facebook page promoting paedophilic content, which, upon investigation, unveiled a broader network of online sexual exploitation. The couple allegedly used online platforms to solicit clients and coordinate meetings, exploiting digital anonymity to facilitate their operations.

In 2019, after extensive investigation, the Crime Branch filed a chargesheet against the couple and 11 others under various sections of the Indian Penal Code (IPC), the Information Technology (IT) Act, and the Protection of Children from Sexual Offences (POCSO) Act. The charges included human trafficking, sexual exploitation of minors, and operating an online prostitution racket.

Types of Evidence Used:

[78] State of Kerala v. Rahul Pasupalan C Anr., Crime No. 1820/2015, Cyber Cell, CBCID, Kerala, decided in 2019.

The prosecution's case was heavily reliant on electronic and digital evidence:

1. Digital Communications: Recovered emails, chat logs, and messages from various platforms demonstrated the coordination between the accused and clients.
2. Social Media Activity: Posts and messages from the Facebook page promoting paedophilic content were crucial in establishing the initial link to the accused.
3. Forensic Analysis: The Centre for Development of Advanced Computing (C-DAC) was engaged to decrypt and analyze encrypted data from seized devices, providing critical insights into the operations of the racket.
4. Testimonies: Statements from victims, including minor girls, corroborated the digital evidence, detailing the modus operandi of the accused.
5. Financial Records: Transactions and bank records were examined to trace the flow of money and establish the financial aspects of the operation.

Grounds for Accepting and Rejecting Evidence:

Accepted Evidence:

Digital evidence was accepted due to proper authentication and certification under Section 65B of the Indian Evidence Act.

Victim testimonies aligned with digital records, strengthening the prosecution's case.

Forensic reports from C-DAC provided credible and detailed analysis of encrypted data, which was pivotal in understanding the extent of the operations.

Rejected Evidence:

The defense's assertion of lack of evidence was dismissed due to the substantial digital and testimonial evidence presented.

The defense highlighted the delay in filing the chargesheet; however, the court acknowledged the complexity of digital evidence analysis as a valid reason for the delay.

Judgment:

The court, upon reviewing the extensive digital evidence and victim testimonies, took cognizance of the serious nature of the offenses. The charges under the IPC, IT Act, and POCSO Act were deemed appropriate given the exploitation of minors and the use of digital platforms for illegal activities.

The judiciary emphasized the importance of adapting legal frameworks to address the evolving nature of cyber crimes. The case underscored the necessity for law enforcement agencies to develop expertise in digital forensics and for the legal system to recognize and admit digital evidence appropriately.

4.5 : Sabu Mathew George v. Union of India (2018) 3 SCC 229 [79]

Facts of the Case:

In 2008, Dr. Sabu Mathew George, a public health activist, filed a writ petition under Article 32 of the Constitution, expressing concern over the proliferation of online advertisements promoting pre-natal sex determination. These advertisements were in direct violation of Section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 (PCPNDT Act), which prohibits any form of advertisement related to sex selection. The petitioner highlighted that search engines like Google, Yahoo, and Microsoft were displaying content that facilitated sex selection, thereby contributing to the declining female sex ratio in India.

The petitioner sought directions from the Supreme Court to ensure the effective implementation of the PCPNDT Act by compelling these search

[79]Sabu Mathew George v. Union of India, (2018) 3 SCC 229.
This case addressed the misuse of online platforms for advertising sex-selective abortion services, leading the Supreme Court to issue directions to search engines to regulate and block such content in compliance with the PCPNDT Act.

engines to remove and block such content. He also urged the Court to mandate the establishment of a mechanism to monitor and prevent the dissemination of such illegal advertisements online.

Types of Evidence Used:

1. Digital Evidence: The petitioner presented screenshots and URLs of search results from the aforementioned search engines that displayed advertisements and content related to sex determination techniques.
2. Affidavits: Affidavits were filed by the Union of India and the respondent search engines, detailing the measures taken to comply with the PCPNDT Act and the Court's interim orders.
3. Expert Reports: Technical reports and expert opinions were submitted to demonstrate the feasibility of implementing filters and blocking mechanisms to prevent the display of prohibited content.
4. Statistical Data: Data highlighting the skewed sex ratio in various parts of India were presented to underscore the societal impact of sex-selective practices and the role of online platforms in perpetuating them.

Grounds for Accepting and Rejecting Evidence:

Accepted:

The Court acknowledged the digital evidence provided by the petitioner, recognizing the presence of content violating Section 22 of the PCPNDT Act on search engine platforms.

Affidavits from the Union of India and the search engines were considered, wherein they detailed steps taken to address the issue, such as implementing keyword filters and removing specific URLs.

Rejected:

The Court found the measures taken by the search engines insufficient, noting that despite assurances, prohibited content continued to appear in search results.

Arguments by the search engines citing technical limitations and the vastness of the internet as challenges to complete compliance were not accepted as valid excuses for non-compliance.

Judgment:

The Supreme Court, in its judgment delivered on December 13, 2017, emphasized the paramount importance of protecting the girl child and upholding the provisions of the PCPNDT Act. The Court directed the Union of India to establish a Nodal Agency responsible for receiving complaints regarding violations of Section 22 of the PCPNDT Act. This agency was tasked with notifying search engines about offending content, which the search engines were then obligated to remove within 36 hours of notification.

Furthermore, the Court introduced the "doctrine of auto-block," mandating search engines to proactively develop and implement in-house mechanisms to automatically block advertisements and content related to sex selection. The Court provided a list of approximately 40 keywords associated with sex determination, instructing search engines to ensure that searches using these terms would not yield any results promoting or facilitating sex selection.
The Court also ordered that the directives be prominently displayed on the policy pages and terms and conditions sections of the search engines' websites to inform users about the prohibition of such content.

This landmark judgment underscores the judiciary's proactive role in adapting legal frameworks to address emerging challenges posed by cyber crimes. By holding search engines accountable for the content displayed on their platforms, the Court reinforced the principle that digital intermediaries have a responsibility to prevent the dissemination of illegal content.

4.6 : Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801[80]

Facts of the Case:

In Shafhi Mohammad v. State of Himachal Pradesh, the Supreme Court of India addressed the admissibility of electronic evidence, particularly when the party presenting such evidence is not in possession of the original device from which the electronic record was generated. The case arose from a criminal proceeding where the petitioner sought to introduce electronic evidence without the certificate mandated under Section 65B(4) of the Indian Evidence Act, 1872. The central issue was whether the absence of such a certificate would render the electronic evidence inadmissible, especially when the party presenting it did not have control over the original device.

Types of Evidence Used:

The primary evidence in question was electronic in nature, including digital records such as video recordings and other electronically stored information pertinent to the criminal investigation. These records were intended to support the prosecution's case and establish the sequence of events related to the alleged crime.

Grounds for Accepting and Rejecting Evidence:

Accepted:

The Court acknowledged that electronic evidence, if authentic and relevant, should not be excluded solely due to procedural technicalities. Recognizing the challenges faced by parties not in possession of the original device, the Court held that the requirement of a certificate under

[80]Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 — This Supreme Court judgment clarified the standards for admitting electronic evidence in criminal cases, emphasizing proper authentication and chain of custody to ensure its reliability in cybercrime trials.

Section 65B(4) of the Indian Evidence Act (1872) is procedural and can be relaxed in the interest of justice.

Rejected:
The Court rejected the notion that the absence of a certificate under Section 65B(4) of the Indian Evidence Act 1872, automatically renders electronic evidence inadmissible, especially when the party presenting the evidence does not have access to the original device.

Judgment
The Supreme Court clarified the legal position regarding the admissibility of electronic evidence, particularly when the party presenting such evidence is not in possession of the device from which the electronic record is produced. The Court held that the requirement of a certificate under Section 65B(4) is procedural and not always mandatory. If the party presenting the electronic evidence is not in possession of the original device, they cannot be expected to produce such a certificate. In such cases, the Court can relax the requirement in the interest of justice. Electronic evidence can be admitted if it is authentic and relevant, even in the absence of a certificate under Section 65B(4), provided the Court is satisfied with its genuineness.
The Court also emphasized that procedural requirements should not impede the delivery of justice. Rigid adherence to procedural norms should not result in the exclusion of crucial evidence.

This judgment holds significant implications for the protection of victims of cyber crime by relaxing the stringent requirements for the admissibility of electronic evidence, the Court has paved the way for victims of cyber crime to present digital evidence more effectively, even when they do not have access to the original devices.

The recognition that procedural technicalities should not hinder justice ensures that perpetrators of cyber crime cannot evade accountability due to rigid evidentiary requirements.

The judgment underscores the importance of integrating technological advancements into the legal framework, ensuring that the justice system remains responsive to the evolving nature of crime in the digital era.

This decision sets a precedent for future cases involving electronic evidence, guiding lower courts to adopt a more flexible and justice-oriented approach when dealing with digital records.

4.7 : Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1[81]

Facts of the Case:

In 2012, Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a writ petition challenging the constitutional validity of the Aadhaar scheme introduced by the Government of India. The primary contention was that the scheme's mandate for collecting biometric data infringed upon the fundamental right to privacy. The Union Government argued that the Constitution did not guarantee a fundamental right to privacy, citing earlier judgments in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962), which held that privacy was not a constitutionally protected right. Given the significance of the issue, a nine-judge bench was constituted to determine whether the right to privacy is a fundamental right under the Constitution.

Types of Evidence Used:

1. The petitioners and respondents extensively analyzed Articles 14, 19, and 21 of the Constitution to interpret the scope of fundamental rights and whether privacy could be inferred from these provisions.

[81]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 — A landmark judgment where the Supreme Court recognized the right to privacy as a fundamental constitutional right, which has major implications for protecting victims in cybercrime cases.

2. Both parties relied on previous Supreme Court judgments. The petitioners cited cases like Gobind v. State of Madhya Pradesh (1975) and R. Rajagopal v. State of Tamil Nadu (1994), which recognized aspects of privacy. The respondents relied on M.P. Sharma and Kharak Singh to argue against privacy as a fundamental right.
3. The Court considered international legal standards and judgments from jurisdictions like the United States, the United Kingdom, and the European Union, where privacy is recognized as a fundamental right.
4. Academic Writings: Scholarly articles and expert opinions were presented to provide a comprehensive understanding of privacy in the modern context, especially concerning technological advancements.

Grounds for Accepting and Rejecting Evidence:

Accepted:

The Court acknowledged that while earlier judgments did not recognize privacy as a fundamental right, subsequent decisions had progressively expanded the scope of fundamental rights to include privacy.

Recognizing the importance of aligning with international human rights standards, the Court accepted the relevance of global jurisprudence in interpreting constitutional rights.

The Court accepted arguments highlighting the challenges posed by technological advancements to individual privacy, emphasizing the need for robust protections.

Rejected:

The Court overruled the judgments in M.P. Sharma and Kharak Singh, stating that they were based on a narrow interpretation of the Constitution and did not account for the evolving nature of rights.

The argument that statutory protections are adequate to safeguard privacy was rejected, with the Court emphasizing the need for constitutional recognition to ensure stronger safeguards.

Judgment

In the landmark case of India **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017),** the Supreme Court recognized the fundamental right to privacy as an essential part of the right to life and personal liberty guaranteed by **Article 21** of the Constitution of India. This interpretation holds significant implications for the protection of women's privacy rights in the digital sphere. While this case primarily focused on the right to privacy, it also addressed the issue of revenge pornography. The Supreme Court acknowledged privacy as a fundamental right under the Indian Constitution in this vital ruling. During the privacy discussions, the Court highlighted that the non-consensual distribution of intimate images or videos, commonly known as revenge porn, constitutes a serious violation of an individual's privacy rights.

The court emphasized that individuals have a reasonable expectation of privacy regarding their personal and intimate images. It recognized that the unauthorized dissemination of private information can lead to considerable harm, such as emotional suffering, reputational damage, and violations of dignity. The ruling stressed the need for legal measures to address revenge pornography and protect individuals from privacy infringements.

Although the ruling did not provide specific guidelines or criteria regarding revenge pornography, it established a foundation for recognizing the importance of privacy in tackling this issue and raising awareness. This has opened avenues for subsequent legal progress and discussions around addressing revenge porn and providing remedial measures for affected individuals.

4.8 : Shreya Singhal v. Union of India (2015) 5 SCC 1 [82]

Facts of the Case:

In November 2012, two young women, Shaheen Dhada and Rinu Shrinivasan, were arrested in Mumbai for expressing their displeasure on Facebook regarding the shutdown of the city following the death of political leader Bal Thackeray. One posted a comment criticizing the bandh, and the other liked the post. Their arrest under Section 66A of the Information Technology Act, 2000 (IT Act), which penalized sending offensive messages via communication services, sparked widespread public outrage and debates on the misuse of the provision. Although the women were released and charges dropped, the incident highlighted the potential for abuse of Section 66A.

In response, Shreya Singhal, a law student, filed a Public Interest Litigation (PIL) challenging the constitutional validity of Section 66A, arguing that it infringed upon the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Indian Constitution. The case was heard alongside other petitions challenging related provisions, including Section 69A and Section 79 of the IT Act.

Types of Evidence Used:

1. The primary focus was on the language and scope of Sections 66A, 69A, and 79 of the IT Act. The petitioners argued that these sections were vague and overbroad, leading to arbitrary enforcement.
2. The case involved interpreting Articles 14 (Right to Equality), 19(1)(a) (Freedom of Speech and Expression), and 21 (Right to Life and Personal Liberty) to assess whether the IT Act provisions violated fundamental rights.

[82] Shreya Singhal v. Union of India, (2015) 5 SCC 1 — A landmark Supreme Court judgment that struck down Section 66A of the Information Technology Act, 2000, for violating the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution.

3. Judicial Precedents: The Court examined previous judgments on freedom of speech, including cases that delineated the boundaries of permissible restrictions under Article 19(2).
4. International Jurisprudence: Comparative analysis with international standards on free speech and digital rights provided context and supported the arguments for striking down Section 66A.

Grounds for Accepting and Rejecting Evidence:

Accepted:

The Court acknowledged that Section 66A's terms like "grossly offensive" and "menacing" were undefined and subjective, leading to arbitrary application and a chilling effect on free speech.

The provision did not establish a clear link between the prohibited acts and public disorder, a requirement for restrictions under Article 19(2).

The Court recognized that the broad language of Section 66A allowed for its misuse against innocent individuals, suppressing legitimate expression.

Rejected:

The government's argument that the provision was necessary to prevent misuse of digital platforms was dismissed due to the lack of narrowly defined parameters and safeguards.

The claim that online speech required different standards than other forms of expression was not accepted as a valid reason for the vague restrictions imposed by Section 66A.

Judgment:

On March 24, 2015, the Supreme Court delivered a landmark judgment, striking down Section 66A of the IT Act in its entirety, declaring it unconstitutional for violating Article 19(1)(a). The Court held that the provision was vague, overbroad, and had a chilling effect on free speech. It failed to establish a

proximate connection between the restricted speech and public disorder, making it an unreasonable restriction under Article 19(2).

The Court also addressed Sections 69A and 79 of the IT Act. While upholding Section 69A, which allows the government to block online content, the Court emphasized the need for procedural safeguards, including a hearing and reasoned orders. Regarding Section 79, which deals with intermediary liability, the Court clarified that intermediaries are required to remove content only upon receiving a court order or notification from the appropriate government agency.

4.9 : The Prajwala v. Union of India (2015)[83]

Facts of the Case:

In February 2015, the NGO Prajwala, led by social activist Dr. Sunitha Krishnan, brought to the Supreme Court's attention the alarming circulation of videos depicting sexual assaults, including rapes and gang-rapes, on various online platforms. These videos, often recorded by the perpetrators themselves, were being shared widely through social media and messaging applications, exacerbating the trauma of the victims and highlighting the misuse of technology in facilitating and perpetuating sexual violence. The NGO's letter to the Court emphasized the urgent need for systemic interventions to curb such cyber-facilitated crimes and protect the dignity and privacy of victims.

Types of Evidence Used

1. Digital Video Evidence: The primary evidence comprised video clips of sexual assaults that were circulating online. These videos served as stark proof of the crimes and underscored the ease with which such content could be disseminated in the digital age.
2. Affidavits and Official Communications: The Ministry of Women and Child Development submitted affidavits detailing proposed measures, including

[83]Prajwala v. Union of India, Writ Petition (Criminal) No. 194 of 2015 — A public interest litigation in which the Supreme Court directed proactive steps for the removal of online videos depicting sexual violence and emphasized stronger mechanisms to combat cyber exploitation and protect victims' identities.

the establishment of specialized agencies and legislative reforms, to address the issues raised.

3. Policy Recommendations: Prajwala provided a set of recommendations aimed at systemic changes, such as the creation of a National Sex Offenders Registry and the development of victim-centric reporting mechanisms.

Grounds for Accepting and Rejecting Evidence:

Accepted:

The Court acknowledged the authenticity and gravity of the video evidence presented, recognizing it as a manifestation of a broader societal and technological problem that required immediate attention.

The Court took cognizance of the NGO's recommendations, viewing them as constructive inputs for formulating a comprehensive response to the challenges posed by cyber-facilitated sexual crimes.

Rejected:

There were no specific rejections of evidence in this case. However, the Court emphasized the need for a coordinated and multi-faceted approach, indicating that isolated measures would be insufficient to tackle the complex nature of cyber-enabled sexual violence.

Judgment

The case revolves around child pornography and the spread of explicit material online. The Supreme Court has instructed the government to adopt suitable measures in collaboration with internet service providers and social media platforms to obstruct, eliminate, and avert the circulation of such material through various technological methods. In relation to this case, the Supreme Court of India issued several directives aimed at addressing the issue of child pornography and the distribution of explicit content over the internet.

An NGO called Prajwala initiated the case seeking solutions to combat Child Sexual Abuse Material **(CSAM)** available online. The Supreme Court responded appropriately by ordering the government to establish a centralized web portal for reporting incidents involving CSAM. This portal will help relay pertinent information to Internet Service Providers **(ISPs)** to block access to such sites. The court emphasized the necessity of implementing proactive monitoring and blocking strategies to prevent the proliferation of CSAM. It directed the government to set up a specialized reporting system for individuals to report instances of Child Sexual Abuse Material.

This system would enable swift action and cooperation between the government, law enforcement agencies, and ISPs for removing objectionable content. The Supreme Court also called for the establishment of dedicated cybercrime units in every state and Union territory to handle complaints related to CSAM and take necessary action against offenders. Furthermore, the statement underscores the need for specialized training for law enforcement personnel to effectively manage cyber crimes associated with child sexual exploitation. The court recognized the international aspect of CSAM and highlighted the importance of global collaboration in efficiently tackling this issue. The directive encouraged the government to pursue Mutual Legal Assistance Treaties (**MLATs**) and other agreements with other countries to facilitate the sharing of information and evidence concerning offenses related to CSAM.

The Supreme Court also stressed the importance of raising public awareness and education in preventing and responding to CSAM. It mandated the government to conduct campaigns and initiatives aimed at informing the public about the potential risks and consequences of CSAM while promoting responsible use of the internet. The goal of these directives is to strengthen the legal framework and enforcement measures to address the distribution of explicit content and protect minors from online sexual exploitation. This strategy highlights the significance of collaboration among various

stakeholders, including government agencies, law enforcement, internet service providers, and the general public, in effectively addressing this issue.

These cases illustrate the judiciary's commitment to confronting hate speech aimed at women and protecting their dignity and rights. Discriminatory speech directed at women can adversely affect their overall well-being and contribute to the ongoing cycle of gender-based discrimination and violence.

4.10 : Ajay Goswami v. Union of India (2007)[84]

Facts of the Case:

Ajay Goswami, a practicing lawyer, filed a writ petition under Article 32 of the Constitution, expressing concern over the publication of sexually explicit content in leading national newspapers. He argued that such content was easily accessible to minors and could adversely affect their mental and moral development.

Goswami contended that while Article 19(1)(a) guarantees freedom of speech and expression, including press freedom, this right should be balanced against the state's duty to protect children under Article 21 (right to life and personal liberty) and Article 39(f) (directive principle to ensure children are not exposed to material detrimental to their well-being).

Types of Evidence Used

1. Newspaper Articles: Goswami presented examples of articles containing sexually explicit material, arguing that such content was inappropriate for minors.
2. Constitutional Provisions: The petitioner relied on Articles 19(1)(a), 21, and 39(f) to support his argument that the state has a duty to protect children from harmful content.

[84] Ajay Goswami v. Union of India, (2007) 1 SCC 143 — In this case, the Supreme Court dealt with concerns over the availability of obscene content in newspapers and its impact on minors, balancing freedom of expression with the need for regulating access to harmful material.

3. International Conventions: References were made to the United Nations Convention on the Rights of the Child, emphasizing the global commitment to safeguarding children's rights.

Grounds for Accepting and Rejecting Evidence

Accepted:

The Court acknowledged that mechanisms like the Press Council Act, 1978, and Section 292 of the Indian Penal Code already regulate obscene publications.

The Court recognized the state's responsibility to protect children from harmful content but emphasized that this must be balanced with other fundamental rights.

Rejected:

The Court found Goswami's suggestions—such as mandatory warnings on newspapers and separate packaging for certain content—to be impractical and lacking in specificity.

The Court held that existing laws were sufficient and that imposing further restrictions could infringe upon the freedom of the press.

Judgment

In this case, the Supreme Court analysed the matter of transmitting indecent messages through electronic communication. As per the Indian Penal Code (IPC), the act of transmitting lewd or indecent messages via email, SMS, or any other means is subject to legal consequences, as determined by the court. The court emphasised that the right to freedom of speech and expression is not applicable to speech that is considered obscene or offensive.

4.11 Yogesh Prabhu v. State of Maharashtra (2015)[85]

Facts of the Case

In 2009, Sonali Asoka Sawai, a journalist, befriended Yogesh Prabhu through the social networking site Orkut. Their acquaintance soured after a face-to-face meeting, leading Sawai to sever ties. Subsequently, she began receiving

emails containing vulgar comments and obscene images on multiple dates in March 2009.

Investigations revealed that these emails originated from IP addresses linked to Prabhu's workplace. Further, a fake profile of Sawai was created, leading to unsolicited calls and messages, causing her significant distress.

The Cyber Crime Investigation Cell (CCIC) traced the emails to Prabhu's office laptop. Upon confrontation, Prabhu confessed to creating the fake email ID and sending the obscene content.

Types of Evidence Used

In this case, a combination of digital, oral, and documentary evidence was presented to establish the guilt of the accused beyond reasonable doubt. The effective use of technology-driven evidence became pivotal in securing the conviction.

1. Digital (Electronic) Evidence:

The most critical category of evidence in this cyber crime case was electronic data. The Cyber Crime Investigation Cell (CCIC) traced the origin of the obscene and threatening emails sent to the victim through IP address mapping. These IP addresses were linked directly to the office network used by the accused. Furthermore, the accused's office laptop was seized and subjected to forensic analysis. The forensic report confirmed the presence of

[85] Yogesh Prabhu v. State of Maharashtra, (2015) Cri. Bail Appl. No. 2733 of 2015 (Bombay High Court) — This case dealt with the misuse of social media platforms to defame and harass a woman, where the Bombay High Court addressed bail and cybercrime implications under the Information Technology Act, 2000.

deleted obscene images, fake email account credentials, and remnants of messages and images that had been transmitted to the victim. This technical evidence was authenticated and presented in accordance with the standards under Section 65B of the Indian Evidence Act, 1872, making it admissible in court.

2. Oral Evidence (Witness Testimonies):

Oral testimonies played a supporting role in reinforcing the digital trail. The victim, Sonali Sawai, gave a detailed account of the harassment, describing the emotional and psychological trauma she experienced. Her testimony was consistent and credible, lending substantial weight to the prosecution's narrative. In addition, colleagues of the accused confirmed his access to the specific workstation and the internet at the given times when the offensive emails were sent. An expert witness, Sonali Mistry—a forensic analyst—testified regarding the analysis conducted on the seized laptop, explaining how the deleted materials were retrieved and matched to the email activity.

3. Documentary Evidence:

Copies of the obscene emails, screenshots of the fake profile, and call data records were submitted to the court as documentary evidence. These records provided a visual and tangible dimension to the digital offenses committed by the accused. The police also prepared a detailed panchanama (record of seizure), which documented the recovery of the laptop and the steps taken during investigation. The authenticity and chain of custody of these documents were maintained meticulously, ensuring their reliability.

Grounds for Accepting and Rejecting Evidence

Accepted:

The court emphasized the strength of circumstantial evidence, referencing precedents like Hanumant v. State of Madhya Pradesh and State of Uttar Pradesh v. Ashok Kumar Srivastava. The chain of events—IP tracing, laptop seizure, and email retrieval—pointed conclusively to Prabhu's guilt.

The recovery of deleted obscene files and traces of the fake profile from Prabhu's laptop provided compelling evidence.

Prabhu's willingness to provide the email account password and the subsequent retrieval of incriminating emails reinforced the prosecution's case.

Rejected:

The defense contended that the absence of eyewitnesses weakened the case. However, the court held that digital footprints and forensic evidence sufficed in establishing guilt beyond reasonable doubt.

The defense suggested that the complaint stemmed from personal vendetta due to a failed relationship. The court dismissed this, noting that Sawai named Prabhu only after thorough investigation pointed to him.

Judgment

In its judgment, the 37th Metropolitan Magistrate's Court, Mumbai, held the accused, Yogesh Pandurang Prabhu, guilty of cyberstalking and digital harassment under Section 66E of the Information Technology Act, 2000, and Section 509 of the Indian Penal Code. The court emphasized that the dignity and modesty of a woman must be protected not only in the physical realm but also in the digital space, which is increasingly becoming a domain of interaction, expression, and unfortunately, exploitation.

The court thoroughly evaluated the digital evidence presented by the prosecution. It found that the chain of circumstantial evidence—ranging from the IP address logs, email records, forensic analysis of the seized laptop, and the accused's own admission of access to the fake email account—formed a complete and unbroken link establishing the culpability of the accused. The recovery of deleted obscene images and offensive messages sent to the complainant left little room for doubt. The court ruled that the accused had intentionally used a computer resource to violate the privacy and modesty of the victim, thereby satisfying the ingredients of both penal provisions.

Accordingly, the court sentenced the accused to three months of simple imprisonment and imposed a fine of ₹10,000 under Section 66E of the Information Technology Act. Additionally, the accused was sentenced to one month of simple imprisonment and a fine of ₹5,000 under Section 509 of the Indian Penal Code. The court directed that both sentences would run concurrently. The judgment sent a strong message that misuse of digital platforms to violate an individual's dignity would be dealt with firmly under the law.

The court underscored that the protection of individuals, especially women, in cyberspace is a constitutional necessity, and the judiciary must adapt to the challenges of the digital age by using available forensic and technological tools to ensure justice. This landmark verdict not only provided justice to the victim but also laid down an important precedent for the prosecution of cyberstalking and online harassment in India.

4.12 : State of Tamil Nadu v. Suhas Katti (2004)[86]

Facts of the Case

This case marks a watershed moment in Indian cyber law jurisprudence, as it was one of the first cases in India to secure a conviction under the Information Technology Act, 2000. The facts of the case revolve around a complaint filed by a woman (name withheld for privacy) who was subjected to severe online harassment and defamation by the accused, Suhas Katti. The victim had earlier refused a marriage proposal from the accused, after which he began harassing her using electronic media.

Suhas Katti created fake Yahoo message group IDs and posted obscene and defamatory messages targeting the complainant. He not only published vulgar material but also included her phone number, inviting strangers to contact her for sexual favors. As a result, the woman received numerous offensive

[86]State of Tamil Nadu v. Suhas Katti, Cyber Crime Cell Case No. 407/2004 (Metropolitan Magistrate Court, Egmore, Chennai) — This was one of the first cases in India where conviction was secured under the Information Technology Act, 2000, involving cyberstalking and harassment through email and online forums.

and unsolicited calls, causing her immense psychological trauma and societal embarrassment.

The victim reported the matter to the Cyber Crime Division of Chennai police in February 2004. The case was swiftly taken up and charges were filed under both the Indian Penal Code and the Information Technology Act. The case gained national significance as it tested the applicability of new cyber laws in protecting women from online abuse.

Types of Evidence Used

The prosecution relied on a combination of electronic and testimonial evidence to prove the guilt of the accused:

1. Electronic Evidence:

The primary evidence included the electronic trail left by the accused. Investigators retrieved the IP address from which the offensive emails and Yahoo group messages were posted. This IP address was traced back to a cyber café frequently used by the accused. Logs maintained by the café confirmed his presence on the dates when the messages were posted.

2. Digital Forensics:

The hard disks of the computers used in the café were seized and analyzed. Deleted browsing histories and cached data confirmed that the accused had logged into the fake Yahoo groups and posted the objectionable messages. Experts provided detailed forensic reports, which were admitted in court under the procedural safeguards of Section 65B of the Indian Evidence Act.

3. Oral Testimonies:

The complainant provided a consistent and emotional testimony outlining the nature of the harassment and its impact on her personal and professional life. Witnesses, including the owner and staff of the cyber café, corroborated that the accused had used their systems during the relevant period.

4. Documentary Evidence:

Printouts of the Yahoo messages, email communications, and call records showing the influx of obscene phone calls to the complainant were submitted. The chain of custody for digital devices and printouts was carefully maintained to uphold their admissibility.

Grounds for Accepting and Rejecting Evidence

Accepted

The court accepted the electronic evidence after ensuring compliance with Section 65B of the Indian Evidence Act, which governs the admissibility of digital records. The prosecution submitted valid 65B certificates from forensic authorities, affirming the authenticity and integrity of the electronic data. The IP address trace and cyber café logbook were cross-verified and found reliable.

Rejected

The court rejected the defense's contention that the accused was being falsely implicated due to a personal grudge. The judge held that the technical trail—such as unique login times, matching IP addresses, and the presence of his credentials—could not have been fabricated and provided irrefutable proof of his involvement. No counter-evidence was offered by the defense to cast reasonable doubt on the prosecution's claims.

Judgment

In a significant step toward addressing cyber crimes in India, particularly those targeting women, the Metropolitan Magistrate Court in Chennai delivered its judgment in State of Tamil Nadu v. Suhas Katti on 5th November 2004. The court carefully examined the facts of the case, giving considerable weight to the electronic and oral evidence presented by the prosecution. It was established that the accused, Suhas Katti, had created false identities and posted obscene and defamatory content about the complainant on a Yahoo message group, and had maliciously shared her phone number to invite indecent proposals from strangers. The court recognized this conduct

as a deliberate act of online harassment and defamation that seriously impacted the complainant's dignity and safety.

Consequently, the court convicted Suhas Katti under Section 67 of the Information Technology Act, 2000, for publishing obscene material in electronic form, along with Sections 509 and 292 of the Indian Penal Code, relating to insulting the modesty of a woman and circulating obscene content, respectively. The court imposed a sentence of two years of rigorous imprisonment along with a monetary fine. Notably, the entire trial was conducted and concluded in a span of seven months, which was lauded as an example of judicial efficiency and responsiveness in cyber crime matters.

Through this judgment, the judiciary not only provided justice to the victim but also set a precedent by acknowledging the power and reach of digital evidence in prosecuting cyber offences. It was an early but decisive assertion that online misconduct—especially against women—would not go unchecked in the eyes of the law. The verdict stands as a landmark in Indian legal history and a foundation for future enforcement of laws protecting individuals from cyber harassment and abuse.

4.13 : Shamsher Singh Verma Vs State of Haryana (2016)[87]

Facts of the Case

In the case of Shamsher Singh Verma v. State of Haryana, the appellant was accused of sexually assaulting his minor niece, leading to the registration of FIR No. 232 on October 25, 2013, at Police Station Civil Lines, Kaithal. The charges framed against him included offenses under Sections 354A and 376 of the Indian Penal Code (IPC) and Sections 4 and 12 of the Protection of Children from Sexual Offences Act, 2012 (POCSO Act). During the trial, after the examination of prosecution witnesses and the recording of the appellant's statement under Section 313 of the Code of Criminal Procedure (CrPC), the defense sought to introduce a compact disc (CD) as evidence. This CD

[87] Shamsher Singh Verma v. State of Haryana, (2016) 15 SCC 485 — The Supreme Court clarified the admissibility of electronic records under Section 65B of the Indian Evidence Act, crucial in cybercrime cases.

allegedly contained a recorded conversation between the victim's father, the appellant's son, and his wife, which the defense claimed would demonstrate that the allegations were motivated by a property dispute within the family.

Types of Evidence Used

The primary piece of evidence in question was the compact disc (CD) containing the alleged conversation. The defense argued that this electronic evidence was crucial to establishing the context of the familial discord and potential motive for false implication. The CD was intended to be authenticated through forensic analysis, including voice matching by the Forensic Science Laboratory (FSL). The defense filed an application under Section 294 of the CrPC, requesting the court to admit the CD as evidence and to facilitate its verification by the FSL.

Grounds for accepting and rejecting evidence

Accepted

The apex court emphasized the Importance of the accused's right to a fair trial and the opportunity to present evidence in his defense. The Court held that a compact disc qualifies as a "document" under Section 3 of the Indian Evidence Act, 1872, and its admissibility should not be denied solely based on procedural technicalities. The Court further clarified that under Section 294(1) of the CrPC, it is not mandatory for the accused or the complainant to personally admit or deny the genuineness of a document; such admissions or denials can be made by their legal representatives.

Rejected

The trial court and the High Court initially rejected the defense's application to admit the CD into evidence. The courts reasoned that the conversation recorded on the CD occurred after the alleged incident of molestation and, therefore, was not directly relevant to the charges. They also expressed concerns that admitting such evidence could delay the trial proceedings.

Judgment

The Supreme Court allowed the appeal, setting aside the orders of the lower courts. It directed that the CD submitted by the defense be admitted as evidence and sent to the Forensic Science Laboratory for authentication, including voice analysis. The Court underscored that denying the accused the opportunity to present potentially exculpatory evidence would be a violation of his right to a fair trial. The judgment reinforced the principle that electronic records, when properly authenticated, are admissible as evidence, and courts must facilitate their examination rather than dismiss them on procedural grounds.

This case is significant in the context of cyber law and the admissibility of electronic evidence in criminal trials. It highlights the judiciary's evolving approach to digital evidence, recognizing the importance of such materials in ensuring justice. The Supreme Court's decision in this case sets a precedent for the treatment of electronic records, emphasizing the necessity of balancing procedural rules with the fundamental rights of the accused. This judgment contributes to the broader discourse on the role of the judiciary in adapting to technological advancements and protecting the rights of individuals in the digital age.

4.14 : State v. Jayanta Das (2017) (Odisha)[88]

Facts of the Case

In 2012, Jayanta Kumar Das, an RTI activist based in Puri, Odisha, was accused of cyberstalking and defamation. Das allegedly created fake profiles of a journalist's wife on a pornographic website, posting her personal details, including her name, address, and phone number, without her consent. This act led to the victim receiving numerous obscene calls and messages, causing her significant mental distress. The motive behind this act was reportedly to take revenge on the journalist, who had previously exposed Das's alleged illegal activities through his reporting. Following a complaint lodged by the

[88] State v. Jayanta Das, Cr. Appeal No. 21 of 2017 (DCS Court, Khurda, Odisha) — A cyber harassment case involving obscene content on social media, tried under the IT Act and IPC.

victim in July 2012, the Crime Branch arrested Das on September 18, 2012. He was charged under various sections of the Indian Penal Code and the Information Technology Act.

Types of Evidence Used

1. Electronic Evidence: The prosecution presented digital evidence, including the fake profiles created on the pornographic website, which contained the victim's personal information. This evidence was crucial in establishing the direct involvement of the accused in the cybercrime.
2. Forensic Analysis: Experts from the Central Forensic Science Laboratory (CFSL), Kolkata, analyzed the electronic data and confirmed the authenticity of the digital evidence. Their testimony played a significant role in corroborating the prosecution's claims.
3. Witness Testimonies: The prosecution examined 13 witnesses, including the victim, her husband, and forensic experts. Their statements provided a comprehensive account of the events and supported the electronic evidence presented.
4. Documentary Evidence: A total of 55 documents were submitted, encompassing the complaint, investigation reports, and other relevant materials that substantiated the charges against Das.

Grounds for Accepting and Rejecting Evidence

Accepted

In this case, the primary grounds for accepting the evidence rested on the admissibility and authenticity of electronic evidence under Section 65B of the Indian Evidence Act, 1872, which governs the admissibility of electronic records. The prosecution provided a valid certificate under Section 65B(4), affirming the authenticity of the electronic data obtained from the pornographic website. This certificate ensured that the digital material—namely, the obscene and defamatory profile uploaded by the accused—was generated and stored through a lawful computer source and had not been tampered with.

Further, the Central Forensic Science Laboratory (CFSL) expert analysis played a pivotal role in establishing a direct technological link between the IP address and digital device used by the accused and the creation of the fake online profiles. The expert report validated the metadata and content integrity of the images and textual data, thus strengthening the evidentiary value.

In addition to digital evidence, eyewitness testimonies, particularly the victim's own account, were found consistent and reliable. The psychological trauma endured by the victim due to the circulation of her explicit fake profiles corroborated the nature and intention behind the crime. Thirteen witnesses were examined, and their statements aligned with the digital trail, further supporting the prosecution's narrative.

Rejected

The grounds for rejecting any evidence presented by the defense were based on the lack of credible counter-evidence. The accused did not provide any material to disprove ownership or access to the implicated IP address or device. The defense also failed to challenge the procedural integrity of the forensic analysis or the validity of the Section 65B certificate. Moreover, no alternative suspect or plausible motive was suggested by the defense to cast reasonable doubt.

Judgment

On August 4, 2017, the Sub-Divisional Judicial Magistrate (SDJM) Court in Puri convicted Jayanta Kumar Das, sentencing him to six years of rigorous imprisonment and imposing a fine of Rs. 9,000. This verdict marked the first conviction in a cyber pornography case in Odisha. The court found Das guilty under Sections 292 (obscenity), 465 (forgery), 469 (forgery for harming reputation), and 500 (defamation) of the Indian Penal Code, as well as Sections 66C and 67A of the Information Technology Act, which pertain to identity theft and publishing sexually explicit material in electronic form, respectively.

The judgment underscored the judiciary's commitment to addressing cybercrimes, especially those targeting women's dignity and privacy. By acknowledging the psychological trauma inflicted upon the victim and the malicious intent of the accused, the court set a precedent for handling similar cases in the future. This case highlighted the importance of digital evidence in modern legal proceedings and the necessity for the legal system to evolve in response to technological advancements.

4.15 : Manish Kathuria Vs Ritu Kohli (2001)[89]

Facts of the Case

In 2001, Ritu Kohli, a resident of Delhi, became the victim of India's first reported cyberstalking case. An individual named Manish Kathuria impersonated her on the chat platform www.mirc.com, engaging in obscene conversations under her name and distributing her personal telephone number. As a result, Ritu Kohli received numerous unsolicited and obscene phone calls from various parts of India and abroad, causing her significant mental distress and invasion of privacy. Upon realizing the severity of the situation, she lodged a complaint with the Delhi Police, leading to the arrest of Manish Kathuria. At the time, there were no specific provisions in Indian law addressing cyberstalking, so the case was registered under Section 509 of the Indian Penal Code (IPC), which pertains to words, gestures, or acts intended to insult the modesty of a woman.

Types of Evidence Used

1. Electronic Evidence: The primary evidence was the activity logs from the chat platform www.mirc.com, where the accused had impersonated Ritu Kohli and engaged in obscene conversations. These logs demonstrated the unauthorized use of her identity and the distribution of her personal contact information.

[89]Manish Kathuria v. Ritu Kohli, Unreported case (2001) — The first reported Indian cyberstalking case involving online impersonation and harassment under IPC Section 509 and the IT Act, 2000.

2. Telecommunication Records: Records of the numerous obscene phone calls received by Ritu Kohli from various locations corroborated her claims of harassment and established a pattern of abuse stemming from the online impersonation.
3. Witness Testimonies: Statements from Ritu Kohli and individuals who were aware of the harassment provided personal accounts of the impact of the cyberstalking on her mental well-being and daily life.
4. Technical Investigation: The Delhi Police traced the IP addresses used during the unauthorized chat sessions to identify and locate the accused, Manish Kathuria.

Grounds for accepting and rejecting evidence

Accepted

The chat logs from www.mirc.com were accepted as authentic records demonstrating the unauthorized use of Ritu Kohli's identity and the nature of the conversations, which were obscene and defamatory.

The phone call records substantiated the claim that Ritu Kohli received numerous obscene calls, linking the online impersonation to real-world harassment.

The successful tracing of IP addresses to the accused provided a direct link between the online activities and Manish Kathuria, strengthening the prosecution's case.

Rejected

At the time of the incident, India's legislations lacked specific provisions addressing cyberstalking or online impersonation. Consequently, the prosecution could not charge the accused under any cyber-specific legislation, limiting the scope of legal recourse.

Judgment

The Delhi Police arrested Manish Kathuria and charged him under Section 509 of the IPC for outraging the modesty of a woman. This section was applied due to the absence of specific cyber laws at the time. The case highlighted the urgent need for legal reforms to address cybercrimes, particularly those involving online harassment and impersonation. Although the Information Technology Act, 2000, had been enacted, it lacked provisions to effectively deal with cyberstalking. This case served as a catalyst for subsequent amendments to the IT Act, including the introduction of Section 66A in 2008, which addressed sending offensive messages through communication services. Furthermore, the Criminal Law (Amendment) Act, 2013, introduced Section 354D to the IPC, specifically criminalizing stalking, including cyberstalking.

4.16 : Raghuraj Singh v maw Air force Bal Bharti School, (2011)[90]

Facts of the Case

In April 2001, a Class XII student of Air Force Bal Bharti School, Lodhi Road, New Delhi, became the center of a significant cybercrime case. Reportedly, the student had been subjected to persistent teasing by his classmates due to his pockmarked facial appearance. In retaliation, he created a pornographic website titled www.amazing-gents.8m.net using free web hosting services. The website contained sexually explicit content, including derogatory remarks and obscene images, targeting female classmates and teachers by name. This act led to widespread outrage among the school community and the victims' families. The father of one of the affected girls, an Air Force officer, filed a complaint with the Delhi Police's cybercrime cell. Subsequently, the accused was arrested and charged under various sections of the Information Technology Act, 2000, and the Indian Penal Code. Given the accused's age, the case was brought before the Juvenile Justice Board.

[90] Raghuraj Singh v. Maw Air Force Bal Bharti School, (2011) — A case involving cyber defamation and online harassment where the court addressed the misuse of digital platforms to tarnish reputation and issued directions under relevant cyber laws.

Types of Evidence Used

1. Digital Evidence: The primary evidence was the pornographic website itself. Investigators retrieved and analyzed the website's content, which included explicit images and defamatory statements about specific individuals. The website's metadata and hosting details were crucial in establishing the origin and authorship of the content.
2. IP Address Tracing: Cyber forensic experts traced the IP address used to create and upload content to the website. This technical analysis linked the online activities directly to the accused's residence, providing a tangible connection between the crime and the perpetrator.
3. Witness Testimonies: Statements from the victims, their families, and school staff were recorded. These testimonies detailed the emotional distress caused by the website and corroborated the timeline of events leading to the discovery of the site.
4. School Records: Academic and disciplinary records of the accused were examined to understand his behavioural patterns and any prior incidents that might be relevant to the case.

Grounds for Accepting and Rejecting Evidence

Accepted

The website's content was directly accessible and verifiable. The explicit nature of the material and the specific targeting of individuals provided clear evidence of intent to harm and defame.

The IP address tracing provided incontrovertible proof linking the accused to the creation and management of the website. This technical evidence was pivotal in establishing the chain of custody and authorship.

The victims' accounts were consistent and detailed, describing the psychological impact and social repercussions of the online content. These narratives reinforced the severity of the offense.

Rejected

The defense did not present substantial evidence to refute the prosecution's claims. There were no alternative explanations or alibis provided that could challenge the established link between the accused and the website.

Investigations did not reveal any indications that the accused was coerced or manipulated into creating the website, thereby affirming the voluntary nature of the act.

Judgment

The Juvenile Justice Board, upon reviewing the evidence and considering the age of the accused, adjudicated the matter under the provisions of the Juvenile Justice (Care and Protection of Children) Act. The accused was found guilty of creating and disseminating obscene material online, violating Section 67 of the Information Technology Act, 2000, which pertains to publishing or transmitting obscene material in electronic form. Additionally, charges under Sections 292 and 509 of the Indian Penal Code, relating to the sale of obscene books and uttering words or gestures intended to insult the modesty of a woman, were considered. Given the juvenile status of the accused, he was not subjected to conventional imprisonment but was instead sent to a juvenile correctional facility in Timarpur, Delhi. The court emphasized the need for rehabilitation and counselling to prevent recidivism.

4.17 : State of Maharashtra v. Awadhesh Kumar Parasnath Pathak (2024)[91]

Facts of the Case

In the case of State of Maharashtra v. Awadhesh Kumar Parasnath Pathak, decided on April 15, 2024, by the Bombay High Court, the accused, Awadhesh Kumar Parasnath Pathak, was a former Technical Manager at Cosmo Films Limited. He was alleged to have misused his position to access and disseminate sensitive business information stored on a company-issued

[91] State of Maharashtra v. Awadhesh Kumar Parasnath Pathak, 2024 SCC OnLine Bom 660 — Bombay High Court denied anticipatory bail in a cybercrime case involving morphed obscene images.

laptop without authorization. The company accused him of unauthorized access, data theft, and breach of trust. Consequently, charges were filed under Sections 408 (criminal breach of trust) and 420 (cheating) of the Indian Penal Code (IPC), along with Sections 43(b), 66, and 72 of the Information Technology Act, 2000 (IT Act).

The accused contended that since the alleged actions were covered under the IT Act, invoking IPC provisions would amount to double jeopardy. He argued that the IT Act, being a special law, should override the general provisions of the IPC in cases involving cyber offences.

Types of Evidence Used

1. Digital Evidence: The primary evidence included logs and records from the company-issued laptop, indicating unauthorized access and data transfer activities by the accused. This digital trail was crucial in establishing the occurrence of the alleged cyber offences.
2. Employment Records: Documents detailing the accused's role, responsibilities, and access privileges within the company were presented to demonstrate the breach of trust and unauthorized actions.
3. Witness Testimonies: Statements from company officials and IT personnel corroborated the unauthorized access and data breach incidents, reinforcing the prosecution's case.
4. Expert Analysis: Cyber forensic experts analyzed the digital evidence to confirm unauthorized data access and transfer, providing technical validation of the alleged offences.

Grounds for Accepting and Rejecting Evidence

Accepted

The court accepted the digital logs and forensic analysis as credible evidence, establishing a clear link between the accused's actions and the unauthorized data access.

The consistent statements from company officials and IT staff supported the digital evidence, strengthening the prosecution's case.

The cyber forensic experts' analysis provided an objective assessment of the digital evidence, which the court found reliable and admissible.
Rejected

The court rejected the accused's contention that applying both IPC and IT Act provisions constituted double jeopardy. It held that the IPC and IT Act address different facets of the alleged offences, and their concurrent application was justified.

Rejected

The court rejected the accused's contention that applying both IPC and IT Act provisions constituted double jeopardy. It held that the IPC and IT Act address different facets of the alleged offences, and their concurrent application was justified.

Judgment

The Bombay High Court, in its judgment, clarified the interplay between the IT Act and the IPC in cybercrime cases. It held that while the IT Act specifically addresses cyber offences, it does not preclude the application of IPC provisions when the actions in question also constitute offences under the IPC. The court emphasized that certain elements, such as deceit and breach of trust, are not comprehensively covered under the IT Act and thus warrant the application of IPC sections.

The court concluded that the accused's actions amounted to both cyber offences and traditional criminal offences like cheating and breach of trust. Therefore, invoking provisions from both the IT Act and the IPC was appropriate and did not violate the principle of double jeopardy. The court's decision reinforced the judiciary's commitment to addressing cybercrime comprehensively by utilizing all relevant legal provisions.

4.18 : Prakhar Sharma v. State of Madhya Pradesh (2018) [92]

Facts of the Case

In Prakhar Sharma v. State of Madhya Pradesh (2018), the case revolved around a serious instance of cyber harassment and online impersonation. The accused, Prakhar Sharma, was alleged to have created a fake Facebook account using the victim's real name and photograph. The fake account was used to post vulgar, obscene, and defamatory content with the clear intention of tarnishing the victim's reputation. These activities led to severe mental trauma and public embarrassment for the victim, prompting her to lodge a formal complaint with the cyber crime cell.

The prosecution argued that the accused, driven by malicious Intent, misused social media to harass the victim by violating her right to privacy and dignity. The content posted from the fake profile was not only defamatory but also sexually explicit, thereby constituting offences under Sections 66C (identity theft), 67 (publishing or transmitting obscene material in electronic form), and 67A (publishing or transmitting sexually explicit material) of the Information Technology Act, 2000. Additionally, the nature of the posts was such that they also attracted potential offences under the Indian Penal Code (IPC), though the primary charges were framed under the IT Act.

Types of Evidence Used

The case involved both digital and documentary evidence, which were critical to establish the identity of the accused and the extent of the offence:

1. Digital Footprints and Metadata: The IP address logs, timestamps, and device IDs associated with the creation and use of the fake Facebook profile were obtained through cooperation with Facebook. These digital footprints led investigators to the device and internet connection registered in the name of the accused.

[92] Prakhar Sharma v. State of Madhya Pradesh, 2018 SCC OnLine MP 934 — Bail denied for creating a fake Facebook profile with obscene content under IT Act Sections 66C, 67, and 67A.

2. Screenshots and Digital Content: Multiple screenshots of the obscene posts and comments made through the impersonated account were submitted by the victim and witnesses. These formed part of the primary evidence.
3. Expert Opinion and Cyber Forensics: The cyber crime cell's forensic team analyzed the digital devices seized from the accused, including his smartphone and laptop, to verify his connection to the fake account. This analysis included recovery of login credentials and browser history.
4. Witness Testimonies: The victim's statement and testimonies of her friends and acquaintances who saw the posts and confirmed their vulgar nature further strengthened the prosecution's case.

Grounds for Accepting and Rejecting Evidence

Accepted Evidence

The court accepted the IP address tracking and device metadata as credible and scientifically verifiable evidence, directly linking the fake profile to the accused's device.

The testimony of the victim was found consistent and corroborated by digital evidence, especially in relation to the timing and content of the fake posts.

The cyber forensic report provided by the investigators was pivotal. It contained detailed analysis tracing the origin of the account activity to the accused, and the data extracted from the seized devices confirmed his involvement.

Rejected or Contested Evidence:

The defense attempted to claim that the accused's devices could have been misused by another person or hacked. However, this argument lacked substantiation and was dismissed due to lack of alternate evidence.

The defense also challenged the admissibility of screenshots citing lack of certification under Section 65B of the Indian Evidence Act. However, the

prosecution submitted a valid certificate, and the screenshots were accepted as secondary evidence.

Judgment

The Madhya Pradesh High Court, while hearing the bail application of the accused, took a strong stance against cyber offences, particularly those that target women's dignity and safety in the digital space. The court noted that the misuse of personal photographs and identity to create a fake online profile not only invades privacy but also causes irreparable harm to the reputation and mental well-being of the victim.

Considering the gravity of the allegations and the prima facie evidence against the accused, the court denied bail. It emphasized that offences under Sections 66C, 67, and 67A of the IT Act are serious in nature and reflect a growing trend of digital abuse. The court observed that such acts not only violate the law but also exploit technological platforms to perpetuate gendered harassment.

By refusing to grant bail, the court reinforced the idea that cyber crimes, especially those involving identity theft and sexual harassment, must be treated with the same seriousness as physical crimes. The judgment reflected a victim-centric approach and a commitment to upholding women's digital safety and dignity.

This case is a crucial case that highlights how the Indian judiciary is evolving to respond effectively to the challenges posed by cyber crimes. The case demonstrates that the courts are willing to rely heavily on digital evidence and expert opinions to ensure justice for victims. It also shows how identity theft and obscenity over social media are being taken seriously by law enforcement and the judiciary alike. The case stands as a strong precedent affirming the judiciary's role in creating a safer digital environment, especially for women who are disproportionately targeted by such crimes.

4.19 : Archana Sharma vs State of NCT Of Delhi & Ors. Aka Bois Locker Room (2020) [93]

Facts of the Case

The Bois Locker Room case emerged in May 2020, when screenshots of a private Instagram group chat called "Bois Locker Room" went viral on social media. The group consisted of teenage boys from Delhi, who allegedly shared sexually explicit and offensive messages about schoolgirls, including sharing images, making derogatory remarks, and discussing plans to exploit and harass girls. The messages were vulgar, misogynistic, and indicative of online sexual harassment and cyberbullying.

Archana Sharma, a social activist and lawyer, filed a Public Interest Litigation (PIL) in the Delhi High Court, seeking a thorough investigation into the matter and demanding action to protect the victims from further harm. The case highlighted the darker side of social media platforms where minors can perpetrate cyber crimes like sexual harassment, stalking, and defamation with relative anonymity.

The Incident sparked a nationwide debate about online safety for minors, the responsibility of social media platforms, and the adequacy of existing laws to tackle such cyber offences. It also revealed the vulnerabilities of victims in the digital space and the urgent need for judicial intervention to ensure justice and preventive measures.

Types of Evidence Used

The investigation and judicial proceedings relied on several forms of evidence:

1. Digital Chats and Screenshots: The primary evidence comprised screenshots of the Instagram chat group, which displayed the offensive messages and images exchanged by the accused boys.

[93] Archana Sharma v. State of NCT of Delhi C Ors., W.P. (CRL) 1084/2020, Delhi High Court — Bois Locker Room case involving obscene Instagram chats; court monitored cybercrime investigation.

2. Forensic Analysis: Cyber forensic experts examined the Instagram accounts involved, tracking IP addresses, timestamps, and digital footprints to verify the authenticity of the conversations and the identities of the participants.
3. Social Media Data: Information obtained from Instagram under legal orders helped establish the creation, membership, and activity patterns of the group.
4. Victims' Statements: Though indirect victims, the girls targeted in the group were given the opportunity to submit statements and affidavits detailing the psychological trauma and harassment they faced.
5. Expert Testimony: Experts in cyber law and psychology were consulted to understand the impact of such cyberbullying on victims and the legal implications of digital sexual harassment.

Grounds for Accepting and Rejecting Evidence

Accepted Evidence:

The court accepted the screenshots of the chat group as crucial evidence, as they were supported by metadata and corroborated by forensic analysis. Cyber forensic reports were accepted to confirm the accounts' authenticity, the timing of messages, and the digital trail leading to the accused minors. Statements by victims and social activists were considered to establish the impact and gravity of the offence.

The court relied on expert opinions regarding cyber harassment and its psychological effects on victims, reinforcing the need for strict judicial measures.

Rejected Evidence:

The defense challenged the admissibility of screenshots, citing possible tampering or misinterpretation. However, the presence of forensic certification and corroboration with server data led to rejection of such claims.

Attempts to minimize the offence as “boys joking” or “non-serious talk” were dismissed by the court, emphasizing the harmful effects of such behaviour and the intent behind it.

The argument that the accused were minors and thus not fully responsible was considered but did not absolve them of the consequences, as the court focused on rehabilitation and deterrence.

Judgment

The Delhi High Court took cognizance of the case’s sensitive nature, recognizing the urgent need to address cyber harassment, especially of women and girls, in the digital age. The court underscored the responsibility of law enforcement agencies to conduct a swift and thorough investigation, utilizing advanced cyber forensic techniques.

The court directed the Delhi Police to file a comprehensive report on the investigation and steps taken to protect the victims. It also emphasized the need for sensitization programs in schools and communities to educate minors about the legal and moral implications of online behaviour.

Significantly, the court highlighted the role of social media platforms in preventing misuse and mandated them to cooperate with authorities for timely data disclosure. The judgment stressed that the anonymity of cyberspace cannot be a shield for perpetrators of sexual harassment or any cyber crime.

While the accused were minors, the court balanced the need for punishment with rehabilitation, encouraging interventions that include counseling and awareness programs to prevent recurrence. It affirmed that the judiciary plays a pivotal role in creating a safe digital environment by reinforcing the applicability of existing cyber laws, such as the IT Act, 2000, and relevant IPC provisions.

The judgment reinforced victim protection by directing the authorities to ensure privacy and dignity of the victims during investigation and trial, thus affirming a victim-centric judicial approach.

The Bois Locker Room case represents a landmark moment in India's judicial response to cyber crime against women and minors. This case highlights how judicial intervention is crucial not only in punishing offenders but also in creating awareness, strengthening cyber forensic capabilities, and urging social media platforms to act responsibly. Ultimately, it underscores the judiciary's vital role in protecting victims from cyber crime and promoting a safer online environment, especially for vulnerable sections of society.

4.20 : Summary

The role of the judiciary in reducing cybercrime against women and children in India is critically important. Through its rulings, interpretations, and mandates, the judiciary has greatly impacted the legal framework and supported the welfare of victims. The judiciary's proactive approach in recognizing the seriousness of cybercrime and its implications for the well-being of women and children has been vital in addressing this evolving threat.

The judiciary's commitment to upholding justice, safeguarding rights, and promoting a safer digital landscape has led to significant advancements in the battle against cybercrime. It has played an essential role in strengthening the legal framework and facilitating effective enforcement of laws related to cyber offenses by interpreting existing legislation in a way that includes such offenses and providing guidance to governmental and law enforcement bodies.

Despite the positive actions taken by the judiciary, challenges remain. The evolving and adaptive nature of cybercrime requires an approach that continuously develops. Ongoing efforts are needed to enhance awareness, skill development, and cooperation among various stakeholders, including the judiciary, law enforcement agencies, governmental bodies, and non-governmental organizations. [94]

[94] Sanyogita and Sibgh "Role of Judiciary in Curbing Cybercrimes" Commonwealth L. Rev. J., Vol. 9 (2023)

Chapter-5

Challenges In Victim Protection And Support Mechanisms

5.1 : PSYCHOLOGICAL AND SOCIAL IMPACT ON VICTIMS

5.1.1 : Psychological and Emotional Factors:

With globalization and modernization, the family structures across different countries have transformed. In India, where joint families have been a common practice, this has been disrupted by the migration of rural individuals to urban areas in search of employment. This migration has contributed to the rise of nuclear families, making the privacy and security of family members a key concern. Historically, there existed a culture of sharing and care that has faded due to nuclear family setups and work obligations, leading to more superficial and less substantial connections among family members and neighbours.[1]

Due to the pressures of work, individuals often lack time for each other, even if they live under the same roof. This prevailing sense of loneliness drives many to engage on various social networking and dating platforms, increasing their susceptibility to cybercriminal activities. In India, the workforce participation rate for women is significantly lower than that for men, with only **33%** of women being part of the workforce compared to **67%** of men. This statistic suggests that homemakers, in particular, are more vulnerable to feelings of solitude, becoming isolated as most family members are absorbed in their careers, which raises the likelihood of depression among women. Women who are primarily homebound often seek external sources of support to combat their feelings of isolation and despair. This tendency increases their likelihood of trusting and relying on complete strangers. [95]

---

[95] Ravi Krishnani, 'Indian Women: No Friends Online' [2015] 32 World Policy Journal 85.
Manya Rathore, 'Share of participation at work across India from 2014 to 2023 by gender' (Statista, 5 March 2023)
https://www.statista.com/statistics/1043300/india-work-participation-by-gender/ accessed 16 March 2023.
D. Halder C K. Jaishankar, Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations (Information Science Reference, IGI Global 2011).

With modern technology at their disposal, social media platforms facilitate interaction with unknown individuals. In an attempt to alleviate their loneliness and the fear of missing out, women tend to engage in chatting, messaging, and video calls, not only with friends but also with strangers, which serves as a form of emotional release. In these vulnerable moments, women frequently disclose sensitive information regarding their homes, family members, property, and banking details. Once this information is obtained, perpetrators can exploit it to commit the aforementioned cybercrimes as well as severe sexual offenses.

5.1.2 : Sociological Reasons:

Throughout the years, the honour and respectability of a family have often rested on its female members. When a rape occurs, society tends to victimize the woman and her family more than the perpetrator. The patriarchal nature of most societies continues to persist, despite some evolution over time, and can still be seen in various forms. This patriarchal framework significantly contributes to the victimization of women in the context of digital crimes.

In India, gender disparities greatly affect nurturing behaviours. A girl is often expected to be submissive and obedient, whereas boys are encouraged to be strong and tough. Due to the fear of stigma, women are conditioned to keep their voices silent. As a result of these behavioural norms, when they experience such crimes, they tend to conceal them from their families, and often, family members also discourage their voices from being heard. [96]

[97]A report on the reporting of cyber-crimes by the NGO Centre for Cyber Victim Counselling included 73 participants, of which 60 were women and 13 were men. These responders, representing different regions of India, are technologically savvy, possess some computer skills, and actively engage on social networking

[96] D. Halder C K. Jaishankar, 'Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India' [2011a] 6(4) Victims and Offenders 386

[97]The Centre for Cyber Victim Counselling conducted a study with 73 people from across India, most of whom were women. Many had faced cybercrimes like receiving explicit threats or having their accounts hacked. However, only a few women actually saw themselves as victims or reported the incidents, often because of social stigma or simply not realizing they had been targeted.

sites in the digital realm. They have faced various forms of victimization, such as receiving threatening emails with explicit content and having their profiles hacked. However, not all 60 female respondents acknowledged their experiences. The survey revealed that only 35% of the women identified themselves as victims, while 46.7% chose not to report, and 18.3% were unaware that they had been victimized. This highlights that societal challenges lead women to prefer not to disclose their victimization. [97]

5.2 : Challenges in Access to Justice and Legal Remedies

5.2.1 : Absence of Specific Legislation Addressing Cyber Crime[98]

Despite having numerous legal provisions aimed at combating cybercrime, India has not fully succeeded in safeguarding women in the online space. The Information Technology Act, which serves as the primary legal framework against cybercrimes, primarily focuses on economic and commercial matters, as stated in its preamble. Cyberstalking is a serious crime that occurs online. Prior to 2013, there was no specific legislation addressing cybercrime, with laws being introduced only after the **Justice J.S. Verma 2013** committee's recommendations. Stalking was subsequently deemed punishable under **section 354(D) of the IPC.** However, this section defines stalking exclusively as an act perpetrated by men. India requires a distinct and comprehensive law against cybercrime akin to that of the United States.

---

[98] Dr. Monika Jain,"Victimisation of women beneath cyber space in India" April-June 2017, Bharati law review. P.no- 8 (2017)
Cyber Stalking: Challenges in regulating cyberstalking at cyber space. Available at http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-atthe-cyber-space.html.(Last visited on 19th July 2020)
IPC: 354(D)-Stalking of women available at https://www.shoneekapoor.com/ipc-354dstalking/#:~:text=Stalking%20behaviours%20are%20interrelated%20to,a%20man%20against%20a%20woman.(Last visited 19th July 2020)
Cyber Stalking: Challenges in regulating cyberstalking at cyber space. Available at http://www.legalserviceiNdia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html.(Last Visited on 19th July 2020)
Cybercrime against women in India and the laws. Available at https://debaraticyberspace.blogspot.com/search/label/morphing. (Last visited 19th July 2020)

Morphing is a rapidly emerging form of cybercrime in today's world. The alteration of celebrity photos to include nudity or the trolling of political figures through morphing has sparked significant outrage. Legal actions have been initiated against those responsible, and charges have been laid. However, a close examination of the Indian Penal Code (IPC) and the Information Technology Act reveals that the term morphing has never been explicitly defined, nor has the act been categorized as punishable under either statute. Charges are filed under **sections 66, 66E, 67, and 67(A)** of the IT Act, as well as **sections 354 or 509** of the IPC. None of these legal provisions specifically address morphed content, and these sections can only be applied in cases of defamation. Given the insufficiency of protective laws, it will become increasingly challenging to prosecute offenders in the future, particularly as the number of cybercrimes continues to expose the weaknesses in the justice system. These examples illustrate certain inadequacies of Indian cyber laws. The laws in India are outdated and require prompt updates. Regular amendments are essential to keep pace with the ever-evolving landscape of technology. India needs to strengthen its cyber laws to combat hackers and stalkers effectively. Ensuring the protection of women in cyberspace should be our top priority. Comprehensive laws aimed at safeguarding women from various crimes, such as online pornography, email spoofing, and stalking, need to be enacted. Restructuring laws and expediting trials are the most effective strategies to defend ourselves against cybercrimes.[99]

5.2.2 : Challenges Encountered by Law Enforcement and the Judicial System in dealing Cybercrime Against Women

A primary issue is the limited resources available to law enforcement agencies for the investigation and prosecution of cyber crimes. Cyber crimes tend to be

[99] Canadian Centre for Cyber Security. (2021). Cyber threats to Canadian individuals and organizations. https://cyber.gc.ca/en/guidance/cyber-threats-canadian-individuals-and-organizations
Times of India. (2019). India third in cybercrime, Delhi leads in crimes: NCRB. Retrieved from https://timesofindia.indiatimes.com/india/india-third-in-cybercrime-delhi-leads-in-crimesncrb/articleshow/71913252.cms
National Cyber Security Policy 2013. (2013). Retrieved from https://www.mha.gov.in/sites/default/files/ncsp_0.pdf

intricate and require specialized expertise and technology for proper investigation. However, many police departments in India are understaffed and lack the essential resources needed to effectively manage cybercrime cases. This can lead to slow or insufficient investigations and low conviction rates.

Another obstacle is the low incidence of reporting among cyber crimes targeting women. A significant number of women may choose not to report cybercrime incidents due to fears of retaliation, social stigma, or a lack of awareness regarding their rights and the legal options available. This underreporting complicates the ability of law enforcement agencies to accurately gauge the prevalence of cyber crimes against women and to allocate resources appropriately.

The IPC and the Information Technology Act, 2000, outline legal provisions for cyber crimes, yet these may not always be effectively implemented or enforced. There may also be ambiguities or discrepancies in how these laws are interpreted, which can lead to varied outcomes in similar cases.

Lastly, insufficient training for law enforcement personnel and legal professionals presents a substantial challenge in dealing with cyber crimes against women. Many officers may lack the requisite knowledge or skills to manage cyber crime cases effectively, while legal professionals may not possess specialized training in cyber crime law. This deficiency can lead to mistakes during investigations or legal proceedings and contributes to low conviction rates.

Cyber crimes against women in India represent a critical issue that demands efficient responses from law enforcement agencies and the legal system. Nonetheless, addressing these crimes is complicated by several challenges, including resource limitations, low reporting rates, inconsistencies within the legal framework, and insufficient training. [100]

[100] National Cyber Security Policy 2013. (2013). Retrieved from https://www.mha.gov.in/sites/default/files/ncsp_0.pdf

5.2.3 : Challenges Encountered by the Indian Judiciary [101]

The Indian Judiciary encounters numerous obstacles due to its traditional criminal justice framework. Some of the challenges that Indian judges face in addressing cybercrime against women include the following:

1. **Digital Evidence Challenges:** The primary issue in computer-related crimes is that most evidence exists in digital formats. This complexity makes it challenging for investigators to locate and preserve digital evidence, while judges and lawyers also struggle to present it effectively in court. **Section 65(B)** of the Indian Evidence Act poses additional problems when it comes to obtaining evidence from foreign service providers, as these companies typically do not issue certificates. Consequently, courts may have to dismiss such evidence, signalling a need for the Indian legislature to acknowledge this issue and amend the section to align with the demands of the digital age.
2. **Outdated Investigation Methods:** Traditional investigation methods have proven ineffective against cybercrime. With the rising use of information and communication technology (ICT), there is a pressing need for new investigative instruments, which necessitate specialized technological expertise and skills in the areas of investigation, prosecution, and conducting cybercrime trials.
3. **Jurisdictional Issues:** Determining jurisdiction presents a significant challenge for the judiciary when dealing with cyber offenses, which are essentially borderless crimes. In such cases, establishing jurisdiction is a complex matter for the criminal justice system. The United Nations and the Indian government both recognize jurisdiction in cybercrime as a considerable challenge. In this regard, the Supreme Court has instructed the government to develop a unified portal for reporting cybercrime.

[101] Neha K. Bhatt and Pareshkumar D. Dobariya, A Challenging Role of Indian Judiciary at Cyberspace to curb Cybercrime against Women

4. **Lack of Specific Legal Provisions:** There is an absence of dedicated legal protections for individual rights in cyberspace. Although the IT Act of 2000 provides general protections to women victims online, the amendments made in 2008 have not adequately addressed newer forms of cybercrime, which complicates the judicial process in cyber trials. The criminal justice system has considered this issue while drafting national policy and has urged the Indian legislature to reclassify the existing cyber codes.

5. **Practical Challenges:** According to **Section 78** of the IT Act 2000, only police officers of inspector rank are authorized to investigate cyber offenses. This stipulation poses a significant practical challenge and adversely impacts the judicial process, leading to increased case backlogs and hindering the pace of trials. Additionally, the lack of cooperation from service providers represents another major hurdle, as the state has limited control over the internet.

6. **Insufficient Technical Tools and Skilled Personnel:** The judiciary grapples with fundamental issues stemming from a lack of technical tools, a shortage of skilled personnel, and inadequate infrastructure, which complicates court proceedings. In 2017, the Indian parliament addressed the need for training resources for those dealing with cybercrime and also proposed the establishment of a nodal agency dedicated to cyber issues.[102]

There exists a disparity between the advancement of technology and traditional knowledge pertaining to newly emerged cybercrimes, alongside the conventional criminal justice system. Established legal procedures for addressing these new types of online offenses are lacking, and specific legal provisions for such crimes have not been defined. Consequently, judges often encounter numerous challenges during cyber trials and in reaching verdicts. In India, the judiciary has taken on a vital role in ensuring the protection and rights of women in cyberspace. The Indian judiciary has been making efforts to address the shortcomings of the Information Technology Act of 2000. In several cases, the

[102] Ibid

judiciary has safeguarded women's rights in the digital realm. However, the evolving landscape of cyberspace is giving rise to various forms of cybercrime that often go unnoticed. Therefore, there is a pressing need for knowledgeable judges who can effectively manage and adjudicate cybercrime cases in India. Moreover, societal awareness and understanding of individual cyber rights are still notably low, emphasizing the urgent need for increasing public consciousness on this issue. It is essential for all constitutional entities to work diligently to promote awareness about cybercrimes and implement measures to combat these issues. [103]

5.3 : Victim Blaming and Social Stigmatization

Due to a lack of awareness and insufficient support structures for women, many individuals are regrettably uninformed about their rights in relation to cybercrime, which hinders their ability to seek justice or report incidents. A significant obstacle is the general unfamiliarity with the process of reporting cybercrimes. Women may be unaware of which authorities or organizations to contact when facing online harassment or exploitation. In addition to receiving fewer reports, law enforcement and cybercrime units often lack sufficient outreach initiatives and awareness campaigns to inform the public about how to report incidents. This absence of information prevents women from effectively pursuing legal remedies. Many women may not be aware that there are dedicated cybercrime cells or helplines available for addressing internet offenses. For instance, the **National Cyber Crime Reporting Portal** was established to facilitate the reporting of cybercrimes, yet many victims remain unaware of this option. The **National Commission for Women (NCW)** also serves as a key statutory body committed to safeguarding women's rights in India.[9]

---

[103] Ibid

[104] Definition of EXPLOITATION (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriamwebster.com/dictionary/exploitation

DEFNITIONS OF CYBERCRIME – https://cybercrime.gov.in/

National commission for women – http://ncw.nic

Social Stigma:[105] Societal perceptions frequently dissuade women from reporting cyberstalking due to concerns about victim-blaming or stigma, which diminishes the effectiveness of existing laws. In India's patriarchal culture, women often encounter social stigma when they are victimized, especially in cases involving sexual harassment or the dissemination of intimate material. Victims might experience embarrassment or shame that prevents them from coming forward, particularly if they fear being held responsible for the crime or bringing dishonour to their family or community. As a result of this anxiety, women may choose to remain silent and endure abuse without receiving the necessary support or legal protection they deserve. Another significant barrier to reporting cybercrimes or seeking legal remedies is the prevailing cultural and societal norms. Family members or peers commonly advise women who are victims of cybercrimes to overlook the harassment or simply move on, a suggestion rooted in entrenched patriarchal beliefs that downplay the seriousness of the offense and dissuade women from addressing it openly.

To address the issue of lack of awareness among women, the government and non-governmental organizations should establish Public Awareness Campaigns aimed at educating women about cybercrimes, their rights, and the legal protections available to them. These campaigns ought to be accessible, relatable, and comprehensible to women from diverse backgrounds, encompassing various age groups, educational levels, and geographic locations. Initiatives to improve digital literacy should be implemented, especially in rural and disadvantaged areas, to empower women to understand the risks associated with internet use and equip them with the necessary tools to protect their online presence from cyber threats.

In terms of addressing the lack of awareness regarding how to report cybercrimes, it is vital to create easily accessible helplines, websites, and mobile applications that allow women to report incidents of cybercrime without fear of

---

[105]Definition of THREAT (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriamwebster.com/dictionary/threats

judgment. These resources should be widely promoted and available in multiple languages to ensure that women can utilize them with ease.

In the context of social stigma, increasing public awareness is crucial for society to comprehend the severity of cybercrime targeting women and the harsh realities they face. The safety and dignity of women online are jeopardized due to the growing and intricate challenges posed by cybercrime against them. The tactics used by cybercriminals evolve with technological advancements, complicating efforts to prevent these offenses. Examples of online harassment that significantly affect women include cyberstalking, revenge pornography, identity theft, and cyberbullying. Beyond the psychological and emotional distress inflicted by these crimes, victims often face victim blaming and social stigma, which discourages them from reporting incidents of cybercrime. Although legislation such as the Information Technology Act of 2000 has made some strides towards combating cybercrime, there is still much work to be done to ensure women's safety online. Victims often find themselves powerless and hesitant to speak out about their experiences due to insufficient knowledge about their legal rights and a lack of support systems. Simultaneously, a cultural shift is necessary to confront the patriarchal views that fuel online violence against women. Changing societal attitudes is essential to empower more women to report cybercrimes. Ending victim blaming will encourage women to feel more comfortable in coming forward about such offenses. [106]

The proliferation of cybercrimes against women in India has prompted the establishment of a legal framework aimed at addressing these issues. This framework includes various laws and regulations in India, such as the **Information Technology Act of 2000**, the **Indian Penal Code,** and the **Protection of Women from Domestic Violence Act**[107] of 2005. The primary

[106] Definition of TRAUMA (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriamwebster.com/dictionary/trauma
Definition of VICTIM (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/victims
[107]Definition of VIOLENCE (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriamwebster.com/dictio

legislation governing cybercrimes in India is the Information Technology Act, 2000 (IT Act), which was introduced to grant legal recognition to electronic transactions and support e-governance. The IT Act features provisions addressing cybercrimes against women, including hacking, identity theft, and electronic stalking. It also mandates the formation of cybercrime investigation units in each state to both investigate and prosecute such crimes. The Indian Penal Code (**IPC**) serves as the principal criminal law in India and includes provisions regarding crimes against women like rape, sexual harassment, and domestic violence. Amendments to the IPC have introduced clauses related to cybercrimes against women, such as voyeurism, cyberstalking, and the dissemination of sexually explicit materials. Additionally, the IPC prescribes penalties for those who abet cybercrimes targeting women. The Protection of Women from Domestic Violence Act, 2005 (**PWDVA**) is a civil statute offering protection to women experiencing domestic violence, defining the term broadly to encompass physical, sexual, verbal, emotional, and financial abuse. The PWDVA also addresses cybercrimes against women, providing measures against online harassment, stalking, and revenge pornography, and it outlines protection orders, residence orders, and financial compensation for women affected by domestic violence.

• In 2019, an individual received a two-year prison sentence for stalking a woman through social media. He had created fake accounts to intimidate her and had made threats to publish her private photographs online.

- The **National Crime Records Bureau** reported that there were more than 4,000 incidents of cyber crimes against women in India in 2019. Among these, over 1,000 cases involved online harassment and stalking.[108]

[108] The Indian Express. (2018). One cyber crime in India every 10 minutes: As technology races ahead of law, Challenges for police and lawmakers. Retrieved from https://indianexpress.com/article/india/one-cyber-crimein-india-every-10-minutes-as-technology-races-ahead-of-law-challenges-for-police-and-lawmakers-5111887
Kaur, R., C Kaur, R. (2017). Cyber Crime Against Women in India. International Journal of Computer Science And Information Security, 15(6), 90-95. Retrieved from https://ijcsis.org/papers/vol15no6/Vol15

• In 2018, the Supreme Court of India reaffirmed the constitutional legitimacy of **Section 66A** of the IT Act, which addresses the penalties for sending offensive messages via communication services. [13]The Court stated that this section is essential for safeguarding women's dignity and preventing cyber harassment.

The legal framework in India addressing cyber crimes against women serves as an important mechanism for offering protection and justice to female victims. This framework comprises multiple laws and regulations, including the Information Technology Act, the Indian Penal Code, and the Protection of Women from Domestic Violence Act. However, effectively implementing these laws poses challenges, highlighting the need for strengthening the capacity of law enforcement agencies and the judiciary. It is also crucial to educate women about their legal rights and the options available to pursue justice. [109]

Victims and their protection

The Court discussed in detail the safeguarding of witnesses during investigations and trials, referring to victim compensation as stated in **Section 396(2)** of **BNSSS**, previously known as s. **357A(2)** of CrPC, which can be provided by the district legal authority or the State legal authority, as reiterated in the 2012 case of **Nipun Saxena Vs. Union of India**, **2018**[110] the Court noted that the compensation scheme would comprehensively support the rehabilitation and compensation for rape victims, who require immediate counselling, legal and medical assistance, and social and economic reintegration.

Violence against women and girls represents a prevalent violation of human rights that leads to severe physical, psychological, emotional, and social repercussions. The journey of filing complaints within the criminal justice

---

[109] Canadian Centre for Cyber Security. (2021). Cyber threats to Canadian individuals and organizations. https://cyber.gc.ca/en/guidance/cyber-threats-canadian-individuals-and-organizations

[110]Nipun Saxena Vs. Union of India, 2018, 10 SCC 703.

Bureau of Police Research and Development, Crime Against Women, Investigation Techniques (2021-22) India

system can often be challenging and traumatizing for numerous victims for a variety of reasons. Gender bias and discrimination perpetuate misconceptions surrounding this violence, which in turn influences the justice response to these victims from their initial interaction with the Police. As the first point of contact, police officers should be well-versed in the legal framework and should consider the appropriate section under which a First Information Report (FIR) should be filed, ensuring the victim receives support in light of their physical, social, and psychological circumstances. [111]

5.4 : Evaluation of Existing Mechanisms for Victim Support and Their Effectiveness

India has made significant progress in its institutional and legislative frameworks to address cybercrimes targeting women. The Information Technology Act of 2000, particularly Section 66E, addresses violations of privacy, such as capturing and distributing images of an individual's private areas without consent. Section 67 penalizes the sharing of obscene content, like pornographic material disseminated without permission in electronic form. Section 67A imposes harsher penalties specifically related to the publication or transmission of sexually explicit actions. Focusing on child protection, Section 67B prohibits any content portraying children in sexual contexts.

Section 354D of the Indian Penal Code (IPC) criminalizes stalking, which includes cyberstalking, and covers scenarios where a man repeatedly follows or contacts a woman to seek an intimate relationship against her consent. Sections 499 and 500 address defamation, applicable when false allegations are made online that harm a woman's reputation. Criminal intimidation involving threats made online is addressed in Section 503. [112]

---

[111] Bureau of Police Research and Development, Crime Against Women, Investigation Techniques (2021-22) India

[112] Definition of PRIVACY (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/privacy
Definition of PORNOGRAPIC (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/pornographic

The Criminal Law (Amendment) Act of 2013: This amendment introduced stronger penalties for sexual offenses and recognized the seriousness of online harassment and stalking, leading to changes in several Sections of the IPC.

The 2013 Act aimed at preventing, prohibiting, and addressing sexual harassment of women in the workplace can also be used to address online harassment within a professional context, despite its primary emphasis on workplace issues. It offers women avenues for reporting incidents and seeking redress. Amendments to the Indian Evidence Act, 1872, enable the use of electronic documents as acceptable evidence, a crucial aspect in prosecuting cybercrimes. Under Section 63B of the Copyright Act, 1957, provisions exist to protect women from data theft, stating that anyone who knowingly utilizes a computer or an infringing copy of a computer program is subject to punishment. [15] The Protection of Children from Sexual Offences (POCSO) Act, 2012, safeguards the rights of girls, with specific sections addressing various forms of sexual assault: Section 3 for penetrative sexual assault, Section 5 for aggravated penetrative sexual assault, Section 7 for sexual assault, Section 9 for aggravated sexual assault, Section 11 for the sexual harassment of a child, and Section 13 for the exploitation of children for pornographic purposes. [113]

The Indian Constitution guarantees women the right to life, human dignity, and freedom of speech and expression; however, the modesty of women is not adequately protected within the Information Technology Act, 2000. The case of **Ranjeet D. Udeshi v. State of Maharashtra (1965)**[114] is a landmark cybercrime case in India involving the distribution of obscene content over the internet. This

[113] Definition of PREVENTION (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriamwebster.com/dictionary/prevention
Definition of PROHIBITION (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriamwebster.com/dictionary/prohibition
Definition of REDRESS (Merriam-Webster: AmericaC#39; s Most Trusted Dictionary) https://www.merriamwebster.com/dictionary/redress

[114] Ranjit D Udeshi v. State of Maharashtra 1965 AIR 881
The Hicklin test is a legal test for obscenity established by the English case R. v Hicklin.England and Wales High Court of Justice, Queen's Bench Division11 Cox C.C. 19 (1868)

case drew attention to the issues of cyber obscenity, online harassment, and the legal interpretation of indecent or offensive online material. The individual involved was Benjamin Franklin, and the test derived from his name is known as the Hicklin Test. This obscenity standard originated from the English case Regina vs. Hicklin (1868), which dealt with issues pertaining to women's pornography and obscenity, as adjudicated by the Court of Queen's Bench in the UK; the Hicklin test serves as a benchmark for obscenity concerning women's pornography.

In the case of **Shreya Singhal v. Union of India (2015)**,[115] a law student challenged Section 66A of the IT Act after the police arrested two women for posting a Facebook message that criticized the closure of Mumbai following a political leader's death. The women were apprehended under Section 66A for allegedly using abusive language online. In a pivotal ruling in 2015, the Supreme Court of India deemed Section 66A unconstitutional, claiming it violated Article 19(1)(a) of the Constitution's right to free speech. The Court found the provision to be vague and excessively broad, resulting in potential abuse and unwarranted arrests. Although this decision was recognized as a triumph for online free speech, it sparked discussions on the necessity for more stringent laws to protect women from online harassment.

The case of **Nikhil Soni v. Union of India (2015)**[116]addressed online harassment and cyberbullying when Nikhil Soni reported being subjected to online harassment across various social networking platforms. She alleged that a group was targeting her with bullying and spreading hateful content, harming her reputation. The Rajasthan High Court ruled in favor of the petitioner, instructing law enforcement to take rapid action against the cyberbullying. This case

[115] Shreya Singhal v union of India air 2015 SC1523

[116]In Nikhil Soni v. Union of India (2015), the Rajasthan High Court held that the Jain ritual of Santhara, which involves fasting unto death, amounts to suicide and is not protected under the right to religious freedom, as it violates the right to life guaranteed by the Constitution.

underscored the urgent need for more rigorous regulations on social media platforms to prevent harassment.

Suresh N. v. State of Maharashtra (2019)[117]: Cyberstalking and Defamation. A man from Maharashtra, Suresh N., faced charges for posting defamatory content on social media and cyberstalking a woman. The woman asserted that Suresh inflicted significant mental distress and harmed her reputation by creating fake profiles and disseminating false information about her. The court convicted the accused under various sections of the Indian Penal Code (IPC), including Section 66E of the IT Act (violation of privacy), Section 500 (defamation), and Section 354D (stalking).

5.5 : Gaps and Effectiveness [118]

India has the Information Technology Act of 2000. The law was primarily established to safeguard e-commerce and financial institutions from cybercrime threats. It lacks provisions aimed at protecting individuals—women, men, and children—from personal attacks that might occur in the online sphere. The issue of "Internet Crime against women" in India is one that has received limited discussion or attention, leaving many victims to suffer in silence. According to the Information Technology Act of 2000, the term "cyber-crime against women" typically refers to sexual offenses and online sexual abuse, including manipulating images for pornographic purposes, subjecting women to harassment through sexually explicit emails or messages, or engaging in cyberstalking. Consequently, the Indian IT Act included a section on pornography and obscenity in the digital realm, namely section 67 of the act, which has been the basis for many earlier cases. However, India did possess a central law like the Indecent Representation of Women (Prohibition) Act, 1986,

[117] In Suresh N. v. State of Maharashtra (2019), the Bombay High Court addressed issues related to cyber harassment, emphasizing that online abuse and threats, especially against women, must be taken seriously under existing cyber and criminal laws to ensure victims' safety and dignity in digital spaces.

[118] K G. Balkrishnan, 'Speech at seminar on cyber-crimes against women – Public awareness meeting', Maharaja College, Ernakulam [2009

along with sections of the Indian Penal Code, such as 509 and 292, which have been used at times to protect women from such indecent crimes; yet, these sections have become outdated in the contemporary era. The Indecent Representation of Women (Prohibition) Act, 1986, was specifically designed for women's protection by banning publications and advertisements that depicted indecent representations of women. It is important to recognize that the Indian interpretation of obscenity differs significantly from that of Western societies, meaning that any sexual depiction or attire of women might be seen as obscene within Indian culture.

Feminist advocates called for better protection but critiqued the law as it approached crimes against women solely from the perspective of obscenity, imposing a moral framework rather than addressing the broader derogatory aspects of crimes committed against women. As a result, this act did not fulfill its intended purpose due to its foundation in a distinctly Indian notion of gendered morality. The act needed amendments to align its penalties with those outlined in the Information Technology Act and extend its application to digital media. If these proposed amendments had been enacted, India could have established a legal framework specifically targeting the victimization of women through indecent representations, which would have been a significant positive change.[119]

The Indian IT Act was revised in 2008, introducing sections 67A and 67B, which are gender-neutral and criminalize the production, creation, and distribution of obscene and sexually explicit content in digital formats. Sections 67 and 67A together aid in protecting against cybercrimes targeting women, but these provisions only allow for financial penalties and charges against “whoever”

[119] Halder, Debarati, ‘Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986, in the Light of Cyber Victimisation of Women in India’ [2013] 11 National Law School Journal.
Geetanjali Gangoli, Indian feminisms: Law Patriarchies and violence in India (Ashgate Publishing, Ltd. 2012).
Vedkumari, ‘Gender Analysis of the Indian Penal Code’ in Archana Parashar C Amita Dhanda (eds), Engendering law: Essays in honor of Lotika Sarkar (EBC 1999).

commits the offense, indicating that even if a creator produces inappropriate images, they can still be found guilty of the crime.

The current Indian IT law still has gaps, the **first** being that it does not address the "removal or deletion of derogatory content." When an offense like photo morphing occurs and such images are circulated online, the psychological impact on the victim is significant. Therefore, the Act should incorporate measures for victim protection and methods for deleting these images and blocking accounts across the internet.

Secondly, the IT Act does not provide for female investigating officers or specialized Cyber cells for women. It is unfortunate that there is no mention in the current Act of gender-specific assistance for victims. Neither Section 78 of the I.T. Act, 2000 nor Section 80(1) clarifies whether a male or female officer is authorized to conduct investigations, searches, or arrests. The low rate of crime reporting suggests that female victims face societal stigma and fear intimidating police stations and male officers, motivating the need for female police officers trained to handle cyber-attacks.

Thirdly, the Indian IT Act uses the term "whoever commits," which implies that original profile creators who produce, publish, or share images that are deemed overly revealing or conduct seen as "sexually explicit" or "obscene" in conservative societies like India can be implicated. As a result, the language of this section could be construed to target the original creators of the profiles. Consequently, authorities often blame victims for being 'too attractive' in their clothing, suggesting that such attire provoked the offense.[120]

Fourthly, internet service providers and other intermediaries should bear increased accountability. Crimes committed online are hosted by various platforms like Google, Yahoo, Facebook, etc. Many Indians join social media networks based in the U.S., creating accounts with U.S.-based ISPs or engaging in online chats that adhere to American laws and regulations. Victims on these

[120] The Information Technology Act, 2000.
Halder, Debarati, 'Examining the Scope of Indecent Representation of Women (Prevention) Act,

platforms often encounter “strange responses” from the ISPs in addition to the legal and judicial systems. This is due to the fact that these incidents either do not fit the criteria outlined in the ISPs’ policy guidelines or are not deemed illegal under Indian law. An increase in accountability for these sites is needed whenever such offenses occur. Data privacy has also become a major issue, as many apps and websites collect personal information and share it with other companies without individuals' consent, fostering an environment conducive to crime and targeting specific people and institutions. Given that India currently lacks a Data Privacy Law, it is crucial to address this issue from a forward-looking standpoint.

Lastly, there is a lack of consistency in the laws across different nations and no overarching international cyber law that can safeguard all victims and penalize offenders. Given that in today's globalized world, emails, websites, and applications can function from any location worldwide, so too can crimes committed on these platforms, with perpetrators potentially being anywhere and able to commit offenses in India without facing consequence due to the absence of legislation to hold such criminals accountable across borders. Cyberattacks cannot be restricted to local laws; therefore, there is a necessity for international cyber laws to address these scenarios. When foreign websites play a role in perpetrating crimes against not only women but also individuals and organizations in India, issues surrounding the effective implementation of the law arise. [121]

5.6 : The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[122] mark an advancement toward a more inclusive, secure, and accountable online environment. To enhance the safety and reliability of cyberspace, the Central Government has enacted the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, under the authority granted by the IT Act, which mandates that

[121] Halder, Debarati, ‘Examining the Scope of Indecent Representation of Women (Prevention) Act

[122] Cybercrime Against Women, https://pib.gov.in/PressReleseDetailm.aspx?PRID=1881404 accessed 10th july 2023

intermediaries, including social media platforms, adhere to several responsibilities, including the following:

• To display their guidelines, privacy policy, and user agreement on their website and app;

• To inform users of these guidelines and make reasonable efforts to ensure that users do not host, display, upload, modify, publish, transmit, store, update, or share, among other things, any information that belongs to someone else, is obscene, infringes on another's privacy, harasses or insults based on gender, is racially or ethnically objectionable, promotes money laundering, incites violence among different religious or caste groups, is detrimental to children, violates intellectual property rights, impersonates someone else, threatens the unity, integrity, defense, security, or sovereignty of India or public order, impedes investigations, or violates any law;

• When receiving an order from a government agency with lawful authority, to provide information or assistance for prevention, detection, investigation, or prosecution of offenses, or in instances of cyber security incidents;

• To establish a grievance redressal system and address complaints of non-compliance within 72 hours of receiving reports;

• If the intermediary qualifies as a significant social media intermediary (defined as one having over 5 million registered users in India), to further implement due diligence by appointing a Chief Compliance Officer, a designated contact person for continuous coordination with law enforcement, and a resident Grievance Officer, as well as to publish monthly compliance reports. [123]

[123] Cybercrime Against Women, https://pib.gov.in/PressReleseDetailm.aspx?PRID=1881404 accessed 10 july 2023

Additionally, amendments to these rules were issued on **October 28, 2022,** which provide for the formation of one or more Grievance Appellate Committees that allow users to contest decisions made by Grievance Officers regarding such complaints. Furthermore, the Ministry of Home Affairs has launched a **National Cyber Crime Reporting Portal** to allow citizens to report a variety of cybercrimes, with particular attention to those targeting women. [124]

5.7 : Summary

Cyber-crimes are unethical and have the potential to greatly damage the reputation of victims, yet many nations focus only on the sexual dimension of these crimes against women, neglecting non-sexual offenses. There is a need for countries to shift away from the societal influences affecting legislation designed to combat these crimes and ensure proper protection is provided. The fear of reputational damage and social stigma surrounding their families often leads to such crimes being underreported and less acknowledged in public discourse. Both the public and law enforcement, including cyber units, lack sufficient awareness in this area. Frequently, they are unclear about how to respond when a victim seeks assistance after such incidents have occurred. It is evident that the low rates of reporting and the near absence of legal action for offenses beyond obscenity and pornography stem from a widespread lack of understanding among the general public, especially among female victims.

Current laws tend to focus solely on punitive measures such as imprisonment, fines, or compensation to the victim. Instead, legislation should extend beyond mere punishment to prioritize the well-being of victims and their reintegration into society following the trauma inflicted by cyber-crimes. Police officers, cyber

[124] In October 2022, the government updated the IT rules to set up Grievance Appellate Committees, giving users a way to appeal decisions made by online platforms. Alongside this, the Ministry of Home Affairs also launched the National Cyber Crime Reporting Portal to help people, especially women, easily report cybercrimes.

cells, and judges have a crucial role in taking further action, such as ordering the removal of online content that has been shared or posted without consent. Law enforcement personnel should receive specialized training for managing these cases, and cyber units should be established in every police station. Additionally, there should be dedicated hotlines for reporting such grievances. Training in reputation management strategies and appropriate conduct can help victims regain confidence.

Moreover, it should be recognized that merely imposing fines or prison sentences is insufficient to prevent cyber victimization. The challenge is amplified by individuals who create fake identities to track and harass victims using social media or other online platforms. Companies such as WhatsApp, Google, Yahoo, Facebook, Instagram, and Twitter, which largely operate from the United States, display a significant lack of accountability for monitoring the online activities of users who engage in harassment through false identities. It is essential for individuals, especially students, to receive training on utilizing these applications and software to safeguard themselves against such crimes and report any incidents to the appropriate authorities.

Ultimately, the internet presents both benefits and drawbacks, depending on how it is used. While it offers numerous opportunities and attractions, individuals must remain vigilant about their rights and privacy, learning how to effectively use applications and technologies in a responsible and positive way.[125]

[125] Cybercrime Against Women, https://pib.gov.in/PressReleseDetailm.aspx?PRID=1881404 accessed 10th july 2023

Chapter-6

Comparative Legal Study and Best Practices

6.1 : Global Efforts Against Cyber Crime:

To safeguard women from cybercrime, numerous international conventions, conferences, treaties, agreements, institutions, and countries have collaborated at the global level. For instance, the Budapest Convention is the first treaty aimed at providing protection against cybercrime. Various international organizations involved in this effort include the Asia-Pacific Economic Cooperation, the dedicated work of the International Criminal Police Organization (Interpol), the United Nations, and the European Union, while countries such as the USA, Canada, Japan, Australia, South Africa, Sri Lanka, India, and Bangladesh have sought to combat cybercrime by incorporating relevant laws into their national legislation. International cybercrime poses significant challenges to both domestic and international law, along with law enforcement practices, as many nations' existing laws are not equipped to address cybercriminal activities. Consequently, criminals are increasingly using the Internet to evade harsher penalties or the challenges of being monitored. [126]

Both emerging and developed nations, along with industry stakeholders, have progressively acknowledged the serious threats that cybercrime presents to economic and political stability as well as public welfare. However, the diverse nature and forms of cybercrime complicate efforts to tackle these issues. Thus, addressing cybercrime requires cooperation on an international scale. Over the years, various organizations and governments have collaborated regionally and internationally to establish global legal standards and law enforcement practices. One of the most notable recent collaborations involves the United States and China, which are the top two countries identified as sources of cybercrime. Information and Communication Technology (ICT) is essential for ensuring interoperability and security based on global standards. To combat cybercrime,

[126] Nuruddin Khan and Dr. Shobha Gulati International Legislative Framework of Cybecrime, http://journalppw.com

various countermeasures have been put into effect, including legislative improvements, technical methods for tracking crimes on the network, internet content regulation, the use of public or private proxy servers, computer forensic techniques, encryption, and plausible deniability, among others.

The law is an adaptive tool that enables the state to respond to evolving social and security challenges, such as balancing criminal enforcement with privacy rights or defining the responsibilities of service providers. Beyond national laws, international law, often referred to as the law of nations, governs interactions between states in all its forms. Provisions regulating cybercrime exist within both national and international legal frameworks. Interpol, recognized as an international law enforcement body with 184 member countries, was one of the pioneers in addressing computer crime, coordinating law enforcement agencies and creating legislative frameworks while working to enhance international capacities to counter cybercrime. Currently, Interpol maintains four working groups focused on information technology crime: the African, American, Asia-South Pacific, and European Working Parties on Information Technology Crime. Alongside these organizations, a Steering Committee for Information Technology Crime was established to unify the efforts of the regional working parties. Interpol has provided technological support to law enforcement regarding the detection, investigation, and collection of evidence related to cybercrime. In addition to law enforcement measures against cybercrime, Interpol engages in preventative actions, including partnerships with credit card companies to tackle payment fraud by creating a database available on Interpol's website. [127]

The influence of cybercrime on women is primarily psychological rather than physical, even though legislation aimed at protecting women focuses more on physical harm. According to recent data from the US Department of Justice, approximately 850,000 American adults, predominantly women, fall victim to cyber-stalking each year, and 40% of women have experienced violence related to online dating. Several Member States have enacted laws to address cyber

[127] Ibid

violence against girls and women; for instance, the UK, Germany, France, and Malta have established laws criminalizing revenge porn, while Slovenia and Ireland are currently considering similar policies. In 2013, the End Violence Against Women Coalition (EVAW) hosted a discussion regarding the enforcement and prosecution of online "harassment and violence," expressing concerns that the criminal justice system responded to online harassment and violence in a less effective manner than it did for offline incidents. Some participants reported receiving "wholly insufficient police responses" when they attempted to report an internet crime.

In the UK, sharing private sexual videos or images without the consent of the owner to inflict harm on the targeted individuals was criminalized in April 2015, with a maximum penalty of two years in prison. Since this law was implemented, over 200 individuals have been prosecuted, as highlighted in a report released in September 2016. Meanwhile, in 2016, France approved the “Digital Republic Law,” which imposes harsher penalties on those convicted of revenge pornography. Offenders can face a two-year imprisonment or a €60,000 fine under this new law. In 2014, a German court passed similar legislation, making it illegal to keep personal images of an ex-partner after they have requested deletion. [128]

The National Centre for Cyber Stalking Research (NCCR), established in the UK in 2009, aims to provide analysis and research on the prevalence, motivations, impacts, and risk assessments of cyber offenses against women and girls. The institute published findings of a study on the prevalence, nature, and effects of cyber stalking in 2011 and is currently conducting a survey on the effects and frequency of revenge porn. Subsequently, in 2015, a hotline for revenge porn victims was established, receiving about 2,000 calls within its first six months.[129]

[128] Ibid

[129] National Centre for Cyberstalking Research (NCCR), established in 2009 in the UK, has played a key role in researching cyber offenses against women. In 2011, it released a study on cyberstalking, and by 2015, it helped launch a revenge porn victim support hotline, which received nearly 2,000 calls in just six months.

The importance of international treaties, conventions, and protocols related to cybercrime within cyberspace is significant, as they create a regulatory framework for the participating countries. This framework obligates nations to adhere to the rules outlined in these treaties, conventions, and protocols. Below are some treaties, conventions, and protocols that are widely accepted by most countries. [130]

The United Nations is the most recognized international organization globally. The United Nations Commission on International Trade Law (UNCITRAL) is responsible for the harmonization and unification of international trade law. Based in Vienna, UNCITRAL has focused on reforms in commercial law for over 40 years. Its mission is to modernize and align international business regulations. In 1996, UNCITRAL released a Model Law on Electronic Commerce in response to the growing prevalence of electronic commerce and advanced communication technologies in global trade. This initiative stemmed from a Resolution passed by the United Nations General Assembly in 19851, which urged nations and international organizations to take measures to ensure legal certainty amidst the widespread use of automated data processing in international commerce.[131]

A World Summit on the Information Society (WSIS) took place in two phases, with the first in Geneva from December 1 to 12, 2003, and the second in Tunis from November 16 to 18, 2005, coordinated by the United Nations and prominently featuring the International Telecommunication Union.[132] Recognizing the significant potential of information and communication technologies for human development, global leaders expressed their "shared desire and commitment to create a people-centered, inclusive, and development-

[130] Nuruddin Khan and Dr. Shobha Gulati International Legislative Framework of Cybecrime, http://journalppw.com

[131] United Nations General Assembly, Model Law on Electronic Commerce with Guide to Enactment 1996, adopted by UNCITRAL, U.N. Doc. A/RES/51/162 (1996), based on the resolution passed in 1985 encouraging legal measures for automated data processing in international trade.

[132] The World Summit on the Information Society (WSIS), organized by the United Nations and led by the International Telecommunication Union, was held in two phases—Geneva (December 1–12, 2003) and Tunis (November 16–18, 2005)—to address global issues related to information and communication technologies.

oriented information society, where all individuals can create, access, utilize, and share information and knowledge, empowering people, communities, and nations to reach their full potential in fostering sustainable development" during the Geneva Summit in 2003. One of WSIS's objectives was to address the digital divide, which refers to the unequal distribution of the benefits associated with the information technology revolution between developed and developing nations, and within societies. The United Nations Commission on Trade and Development (UNCTAD) serves as the main trade and development agency of the United Nations General Assembly. Since 1998, UNCTAD has been advocating for the significance of information and communication technologies in development, following a special grant allocated by the General Assembly to support and promote electronic commerce initiatives.[133]

6.2 : The Budapest Convention [134]

The European Convention on Cybercrime, held on November 23, 2001, in Budapest, approached cybercrime and international cyber law comprehensively. It stands as one of the most crucial international conventions addressing issues related to cybercrime and electronic evidence. The document was developed in collaboration with the Council of Europe, Canada, Japan, South Africa, and the United States. This Convention is structured into four chapters containing a total of 48 articles. It serves as a global treaty on criminal justice, equipping States with mechanisms for the criminalization of certain computer and internet-based behaviours; establishing procedural law for investigating cybercrime and admitting electronic evidence in criminal proceedings; and fostering international collaboration among law enforcement and judicial authorities concerning cybercrime and electronic evidence. India's position regarding the convention reflects its non-member status, although India supported a separate convention. Furthermore, data sharing with foreign entities is viewed as a violation of the nation's sovereignty, as stated by the Intelligence Bureau. Due to

[133] The 2003 Geneva Summit of WSIS emphasized building an inclusive information society and bridging the digital divide, highlighting the role of technology in sustainable development.

[134] Nuruddin Khan and Dr. Shobha Gulati International Legislative Framework of Cybecrime, http://journalppw.com

an inadequate legislative framework, India's data protection regulations currently face significant challenges and discontent. The legal framework encompasses the following elements:

The Information Technology Act of 2000 (IT Act) includes legislative provisions concerning cyber and IT-related laws in India (such as sections 43A and 72A). Section 43A addresses compensation related to data breaches. Section 72A states that any knowing and intentional disclosure of information without the consent of the individual concerned can lead to imprisonment for a maximum of three years. However, these provisions fail to provide protection against data breaches and do not establish a privacy framework based on individual rights.

Approximately 67 countries have ratified the Convention, and ten international organizations (including the Commonwealth Secretariat, European Union, INTERPOL, International Telecommunication Union, Organization of American States, UN Office on Drugs and Crime, among others) take part in the Cybercrime Convention Committee as either members or observers. The Committee is responsible for overseeing the Implementation of the Convention by the signatories. Nevertheless, since India is not a signatory to the Cybercrime Convention, it is not obliged to modify or implement its domestic laws in accordance with the Convention.

In October 2002, the Commonwealth Secretariat developed a "Model Law on Computer and Computer-Related Crime" for the 53 member nations of the Commonwealth. This Model Law broadened the range of criminal liability for crimes involving the internet and computer systems, along with the unauthorized use of computer-related devices and practices.[135]

[135] Ibid

Within the context of cybercrime, the Model Law also introduced the principle of dual criminality. It suggests that if an individual commits a crime outside of their country, they can be prosecuted if their actions would be punishable under the laws of the country where the crime occurred. This dual criminality concept may lead to prosecution or extradition. Some Commonwealth member countries have utilized the Model Law to draft local cyber legislation.

During their Second Ministerial Conference in Geneva, Switzerland, on May 20, 1998, members of the World Trade Organization (WTO) adopted a declaration regarding global electronic commerce, reflecting the increasing significance of internet commerce in international trade. The declaration tasked the WTO General Council with formulating a comprehensive work programme to assess all trade-related issues emerging from electronic commerce and to submit a progress report to the WTO's Third Ministerial Conference.

The Group of Eight (G8) is composed of eight nations and was mainly concentrated on pursuing high-tech criminals and promoting technical and legislative advancements to combat global computer crimes during the Denver Summit in 1997.

At the Okinawa Summit in 2000, the Okinawa Charter on Global Information Society embraced concepts of international cooperation and harmonization for addressing cybercrime. The G8 affirmed the importance of privacy protection, the unobstructed transfer of information, and security of transactions.[136]

The World Intellectual Property Organization (WIPO), located in Geneva, comprises 179 member states. WIPO aims to "promote the protection of intellectual property worldwide through international cooperation" (WIPO Convention, Article 3). WIPO serves as the steward of 23 international treaties and acts as a platform for developing and regulating global IP policies. With the shift of intellectual property into the digital realm, there is an increasing necessity for protection, as digital formats allow for unlimited perfect copies that

[136] Ibid

can be effortlessly shared across global networks. Consequently, it becomes essential to safeguard online content, including information, music, software, films, business methods, databases, and so forth.

The United Nations Convention against Transnational Organized Crime (UNCTOC) was ratified by the United Nations in 2000. The Palermo Convention obliges signatory nations to establish domestic laws aimed at organized crime groups, along with developing novel procedures for extradition, mutual legal support, and cooperation in law enforcement. Although the treaty does not explicitly address cybercrime, its articles are highly relevant.

Article 34 of the 1989 Convention on The Rights of the Child requires countries to safeguard children from all forms of sexual exploitation and abuse, including prostitution and pornography.

The Protocol to the Convention on the Rights of the Child (Optional Protocol) (2001) addresses the sale of children, child prostitution, and child pornography, building on the CRC Convention. Article 3(1) bans the production, distribution, dissemination, sale, and possession of child pornography, with the Internet mentioned in the Preamble as a means of distributing such material. Article 2(3) provides a broad definition of child pornography that encompasses virtual images of minors. [137]

A Comparative Analysis of Cyber Crime Against Women reveals that sexual cybercrimes transcend boundaries and jurisdictions, making it a global issue rather than one confined to a single country. In cyberspace, foreign nations are typically more proficient in technology and computer science compared to India, which means that understanding the laws, rules, and regulations of various countries can inform and inspire our advancements to meet international standards.[138]

[137] Ibid

[138] Priyal Singh, "Patriarchal Face of Cyber Stalking" 2 International Journal of Law Management and Humanities (2019).

6.3 : United States of America[139]

In the United States, regulations addressing stalking were first formally recognized in the Michigan Criminal Code in 1993. This legal framework introduced the concept of 'harassment' as a part of stalking for the first time. Within this Code, harassment is characterized as "conduct aimed at a victim that includes repeated or ongoing unconsented contact, which would cause a reasonable person to experience emotional distress, and that indeed results in the victim experiencing emotional distress."

Laws concerning online pornography and obscenity also address the use of offensive language and images in electronic communications, classified as a crime under Section 2261A of Chapter 110A, Part 1 of Title 18 USC, which covers issues of dating violence, stalking, and domestic violence against women. Laws prohibit the creation and dissemination of obscene materials as detailed in Chapter 71, Part 1 of Title 18 of the U.S. Code. Section 1801 of Chapter 88, Part 1 of Title 18 USC addresses video voyeurism and its distribution.

The Electronic Communications Privacy Act of 1986 (ECPA) merges the Electronic Communications Privacy Act with the Stored Wire Electronic Communications Act. The ECPA updated the Federal Wiretap Act of 1968, which only dealt with the interception of conversations over traditional telephone lines, not covering digital and other electronic communications. Subsequent legislative acts, including the USA PATRIOT Act, further clarify and revise the ECPA to keep pace with advancements in communication technology and methods, such as easing limitations on law enforcement access to stored communications in certain situations.

[139] Priyal Singh, "Patriarchal Face of Cyber Stalking" 2 International Journal of Law Management and Humanities (2019).
Nuruddin Khan and Dr. Shobha Gulati International Legislative Framework of Cybecrime, http://journalppw.com

General Provisions

The ECPA, in its updated form, protects all wire, oral, and electronic communications during use, transit, and while stored on devices. The Act encompasses email, phone conversations, and electronically saved data.

6.4 : United Kingdom [140]

Cyber stalking

The Protection of Freedoms Act of 2012, which introduced sections 2A and 4A to the Protection from Harassment Act of 1997, acknowledged cyberstalking as a crime in England and Wales. This is in addition to traditional laws related to harassment that involve digital publication. The Protection from Harassment Act of 1997 is considered the primary legislation addressing cyber stalking. According to Section 1 of this Act, "A person must not engage in a course of conduct (a) that constitutes harassment of another individual, and (b) that the person knows or should know amounts to harassment of the other." Section 4 addresses the element of 'fear,' which is necessary to constitute the offense of cyber stalking.

Sexual offences

The Criminal Damage Act of 1977 does not specifically tackle issues related to sexually explicit defamation of women or the violation of their online privacy. The Computer Misuse Act of 1990 prohibits the damaging, altering, or unauthorized access of computer systems or networks. The Theft Act of 1968 addresses the fraudulent use of a victim's identity. The Equality Act of 2010 deals with online harassment, particularly when motivated by sexual intent. Under Section 67 of The Sexual Offences Act, 2003, voyeurism and its distribution without genuine consent are punishable offenses.

[140] Priyal Singh, "Patriarchal Face of Cyber Stalking" 2 International Journal of Law Management and Humanities (2019).

Cyber flashing

The United Kingdom is poised to establish Cyber flashing as a distinct crime under the Online Safety Bill 121 2022-23, which was proposed in the U.K. parliament, with a maximum prison sentence of two years. The objective of defining this as an offense is to enable the Government to keep pace with emerging global crimes over time.

6.5 : Australia [141]

In New South Wales, it is illegal to stalk someone, regardless of whether the stalking occurs online. Section 13 of the Crimes (Domestic and Personal Violence) Act 2007 specifies that the maximum penalty for stalking or intimidation is five years' imprisonment.

Cyber Harassment

Various types of harassment, including hacking, morphing, cloning, and impersonation, are addressed in the Federal Criminal Code Act of 1995, which was amended by the Cyber Crime Act of 2001. Under Sections 477.1, 3, and 2 of the Cyber Crime Act of 2000, unauthorized access or tampering with computer data with malicious intent is punishable. Divisions 477 and 478 of the Criminal Code Act of 1995 were created to safeguard women's profiles on social media and personal websites to prevent them from becoming victims of cybercrime.

Cyber Stalking

Cyber stalking is governed by Section 34A of the Crimes Act of 1900 in the Australian Capital Territory, Section 189 of the Criminal Code Act of 1995 in the Northern Territory, Section 359A of the Criminal Code Act in Queensland, Section 19AA of the Criminal Law Consolidation Act of 1935 in South Australia, Section 192 of the Criminal Code Act of 1924 in Tasmania, and Section 21A of the Crimes Act of 1958 in Victoria. The legal structure for addressing cyber harassment is similarly inadequate. The Information Technology Act of 2000,

[141] Priyal Singh, "Patriarchal Face of Cyber Stalking" 2 International Journal of Law Management and Humanities (2019).

designed to regulate online commerce and facilitate e-governance, fails to effectively tackle cyber harassment or provide sufficient legal protection for victims of this behaviour. While the act criminalizes the distribution of sexually explicit content and cyberstalking, the penalties often tend to be minimal and do little to deter offenders.

6.6 : Effective Strategies for Preventing Cyber Crime Against Women

The incidence of cyber crimes targeting women in India is increasing, making it essential for women to take proactive steps to protect themselves from victimization. Here are some effective strategies that women can implement to safeguard against cyber crimes.

• **Create Robust Passwords**: One of the easiest yet most powerful methods to defend against cyber crimes is to use strong passwords. Ensure that your passwords are at least 12 characters long, incorporating a blend of upper and lowercase letters, numbers, and special symbols. Steer clear of easily guessed passwords such as your name, birthdate, or pet's name.

• **Keep Personal Data Confidential**: Exercise caution regarding the personal information you divulge online, particularly on social media platforms. Refrain from publicly sharing your phone number, home address, or other sensitive information. Additionally, be alert to phishing emails or calls soliciting personal information.

• **Exercise Caution with Social Media**: Social media can serve dual purposes. Although it helps maintain connections with friends and family, it can also harbour instances of cyber crimes. Be discerning about whom you add as friends and avoid posting personal information or sensitive images online. [142]

[142] Gupta, S., C Kapoor, M. (2018). Cyber Crime in India: An Empirical Study on Cyber Crime Awareness among
Women. International Journal of Management Studies, 5(4), 106-111. Retrieved from http://www.aarf.asia/images/short_pdf/1538513964_12.%20PAPER%203

• **Activate Two-Factor Authentication**: Two-factor authentication provides an additional layer of security for your online accounts by necessitating a secondary form of verification, such as a code sent to your phone, in addition to your password. Many widely-used online services, such as email providers and social media networks, offer this feature.

• **Keep Programs Updated**: Ensure that your software, including your operating system and antivirus applications, are current. Software updates often include security fixes that address vulnerabilities that cybercriminals might exploit.

• **Utilize Antivirus Programs**: Antivirus software helps identify and prevent malware and other harmful software from infecting your device. Be sure to install trustworthy antivirus programs and keep them regularly updated. [143]

As more individuals use technology for communication and entertainment, India is increasingly concerned about the issue of sexual harassment in cyberspace. Various forms of cyber harassment include online stalking, sexual solicitation, revenge porn, cyberbullying, and sexual harassment via email, social media, or other digital means. The anonymity provided by the internet has exacerbated the issue, allowing offenders to disguise their identities and evade consequences.

There are several voids that require attention. The current legislation needs to expand its definition of sexual harassment to specifically include online sexual harassment. The existing focus solely on physical sexual harassment in the law should be revised.

Additionally, there is a lack of awareness and training among law enforcement agencies regarding cybercrime, and the Indian police are frequently unprepared to address it. Consequently, cybercriminals are not dissuaded, leading to low conviction rates.

---

[143] Australian Institute of Criminology. (2018). Cybercrime against individuals and businesses. https://aic.gov.au/publications/sb/sb13

In India, incidents of cyber crime targeting women are escalating rapidly, with new offenses such as cyber trolling and cyber bullying emerging. However, the IT Act of 2000 does not encompass these crimes, and the current investigation process is inadequate. The Act fails to offer any solutions for cyber trolling and gender-based bullying, highlighting a significant gap in the legislation. Additionally, cyber stalking is a severe issue that necessitates the establishment of stringent laws through amendments to the IT Act, 2000. Most cyber crimes ought to be classified as non-bailable offenses. There is an urgent need to establish a dedicated cell for investigations, as well as to formulate a distinct law for this purpose. A thorough data protection framework should be integrated into the legislation to enhance its effectiveness. Law enforcement officers must receive specialized training to effectively address cyber crimes against women. Furthermore, the Indian judiciary must play a crucial role in combating cyber crimes against women in the country. The Indian government should pursue bilateral collaborations with other nations to facilitate the exchange of information related to cyber crime. [144]

[144] Outlawing cyber crimes against women in India https://docs.manupatra.in› articles› upload
Dr. Jai Narayan Pandey, Indian Constitution, Central Law Agency, Forty-Three Edition, 2010.

CHAPTER-7

CONCLUSION AND RECOMMENDATIONS

7.1 : Conclusion [145]

In India, a significant number of cyber crimes against women go unreported. Victims of cyber crime have the responsibility to report these incidents so that appropriate action can be taken, which will help reduce the overall crime rate. It is essential that issues pertaining to women are specifically addressed and protected by legislation. Failure to do so may incentivize cyber criminals or stalkers to continue engaging in these deplorable acts. Often, these crimes remain unreported because women are not aware that they are occurring. Therefore, the government should take steps to raise awareness about cyber crimes. Various websites and blogs offer safety tips for women and children using the internet. Despite these resources, cyber crime against women continues to increase. It is recommended that women thoroughly read all instructions prior to using any websites or applications.

Currently, various forms of cyber crime aimed at women are being carried out in India. The importance and necessity of the internet have rendered it an integral part of everyday life for many. Individuals of all ages use the internet, which, while beneficial, also presents certain risks. Cyber crime targeting women is not only an issue in India; it is a global concern. Governments worldwide are increasingly worried about its prevalence. Existing legislative measures aimed at addressing cyber crime are inadequate for effectively tackling the issue. These laws do not fully capture the realities faced by women when they fall victim to cyber crime. The initial step towards providing victims with legal options is to ensure that women's experiences of online threats, harassment, abuse, or intimidation are accurately reflected in regulatory frameworks through amendments to two key laws. Undoubtedly, the Indian Parliament enacted the IT Act, 2000 with the intention of

[145] Mohit and Sanjeev, Cyber Offences Against Women and Legal Protection2023, https://www.thelawbrigade.com

facilitating the fight against cyber crime. However, there are still gaps in Indian legislation, such as:

- The Information Technology Act of 2000 does not define or use the term "cyber crimes," instead specifying and punishing certain offenses. The IT Act of 2000 only addresses a limited number of cyber crimes and does not encompass all forms. Cyber defamation is defined in the Indian Penal Code, but it is not addressed in the IT Act of 2000. If a public good defense is presented, such as the material being of general interest or related to confidential religious matters, sections 67, 67A, 67B, and 67C cannot be asserted to include pamphlets, books, papers, writings, paintings, drawings, representations, or figures in electronic formats.

- Viewing content for personal use does not constitute a violation of any provisions in the IT Act 2000; however, if it can be demonstrated that you have published, shared, or facilitated publication in any electronic format, it could be considered an offense under Section 67.

- Common cyber-crimes such as morphing, cyber stalking, and email spoofing are not categorized as offenses within the IT Act, 2000. [146]

7.2 : Recommendations[147]

- India should ratify a cybercrime convention, such as the Budapest Convention, to comply with international standards and effectively combat such crimes on a global scale, similar to its participation in international treaties addressing organized crime and drug trafficking. A comprehensive approach is necessary that includes education, awareness initiatives, and legislative reform to tackle the issue of cyber harassment in India.

---

[146] Mohit and Sanjeev, Cyber Offences Against Women and Legal Protection2023, https://www.thelawbrigade.com

[147] https://www.researchgate.net/publication/378488323_The_Sexual_Harassment_against_Women_in_Cyber_Space_Concept_Reality_and_the_Law

- The media should take on a greater role in positively representing women and highlighting the risks associated with online abuse to provide better legal protection for victims and ensure accountability for offenders, the legal framework needs to be reformed.

- Establish a detailed legislative structure that specifically addresses online harassment, including clear definitions and penalties for perpetrators, and create an accessible reporting system that ensures the safety and privacy of victims.

- Increased awareness campaigns are essential to educate the public, law enforcement, and the judiciary about the legal limitations and consequences of cybersex harassment, as well as to provide a user-friendly reporting system that guarantees victim safety and confidentiality. Victims of cyberbullying should receive appropriate support and complaint procedures, including counseling and legal assistance. [148]

[148] Ibid

7.3 : Government Initiatives and Policies[149]

The Ministry of Home Affairs initiated the National Cyber Crime Reporting Portal in 2018, providing a platform for citizens to report cyber crimes. This portal allows individuals to report cyber crime incidents, especially those targeting women, while offering information on cyber crime prevention and safety measures. It also facilitates quick action by law enforcement agencies on the cases reported.

Also launched in 2018 by the Ministry of Home Affairs, the Cyber Crime Prevention against Women and Children (CCPWC) scheme allocates financial aid to states and union territories for establishing specialized cyber crime cells focused on cases involving women and children. Furthermore, the scheme includes the establishment of a dedicated cyber forensic laboratory in every state and union territory to support investigations into cyber crime cases.

In addition to these initiatives, the Indian government has implemented several policies aimed at countering cyber crimes against women. The National Policy for Empowerment of Women, introduced in 2001, encompasses provisions for the protection of women's rights in the digital space. This policy highlights the importance of addressing gender-based violence in all its forms, including online, and advocates for the creation of gender-sensitive legislation and policies to tackle these issues.

Launched in 2015, the Digital India initiative seeks to convert India into a digitally empowered social and knowledge economy. This initiative incorporates aspects for promoting digital literacy and raising awareness about cyber security among citizens, particularly targeting women and girls. It also includes efforts to enhance the quality and accessibility of digital

[149] Government of India, Ministry of Home Affairs, National Cyber Crime Reporting Portal, launched in 2018, and Cyber Crime Prevention against Women and Children (CCPWC) Scheme, 2018. See also the National Policy for the Empowerment of Women, 2001, and the Digital India Programme, 2015, for broader frameworks addressing women's digital safety and empowerment.

infrastructure and services, which can help bridge the digital divide and improve technology access for women.

Cybercrime is viewed as one of the paramount challenges facing humanity. However, we have misconstrued the reality; cybercrime has already established a significant presence worldwide. Hacking and data breaches have raised serious concerns among leading intelligence agencies. Cybercrime has transformed into a more covert issue. Given this context, it is crucial to protect the integrity and dignity of women. Cyberspace has created an opportunity for perverts, fraudsters, black market operators, and other anti-social individuals to pursue their agendas. It is vital for national and international leaders, women's rights advocates, and various social service organizations to recognize that cyberspace poses as significant a problem as any other societal issue. India faces a considerable risk of cyber-crimes with an extensive database, tracking everyone and everything will undoubtedly pose a challenge. To keep pace with advancements in data services and internet access, the government must enhance cybersecurity measures strengthening border security or constructing physical barriers would be futile if the real battle is taking place in the virtual realm. Unfortunately, this is the reality. The world is focused on the threat of nuclear war, while the issue of cyber warfare has emerged as an urgent concern. India should strive to protect women and not allow them to become victims amid this chaos. It is wise to embrace the adage, "prevention is better than cure" by developing a robust cybersecurity framework and promoting a healthy digital environment for women, India could take the initiative in combating this menace.

The Internet has the potential to empower individuals at the beginning of the new millennium by granting them access to information and social support regarding their physical and mental health, as well as by fostering digital advocacy for changes in societal and organizational policies. [150]

[150] Cybercrime Against Women in India: Legal Challenges And Solutions, available at https://www.ijlmh.com./ Cybercrime Against Women, https://pib.gov.in/PressReleseDetailm.aspx?PRID=1881404 accessed 10th march2025

Nevertheless, there are risks and hazards that need to be addressed. Online victimization can stem from inadequate information, breaches of privacy, limited communication, online harassment, and cyberstalking. To fully harness the Internet's potential for providing services, it is essential for both individuals and institutions, including e-commerce sites, to understand and guard against the associated risks. While taking precautions and educating oneself on online safety and privacy is crucial, it is not sufficient on its own. The laws of a country typically reflect its societal and moral values, as well as the rules of social conduct. Over the years, technological advancements have progressed at an extraordinary pace, increasing the user base of the internet, computers, and mobile devices, often outpacing the legislation governing them. This rapid change has opened up numerous opportunities for many, yet it has also led to misfortune for others who have been adversely affected in various ways.

Cyber-crimes are unethical and can significantly damage the reputation of their victims; however, many nations tend to acknowledge only the sexual dimensions of such crimes, particularly against women, neglecting non-sexual offenses. Countries still need to shift away from the social perspectives underlying the laws intended to combat these crimes and provide adequate protections. Due to concerns about reputation and the stigma associated with their families, such incidents often go unreported. Public awareness, as well as knowledge among investigative personnel and cyber units, is lacking. These parties frequently do not know how to react or assist when a victim seeks help following an incident. It is acknowledged that the primary reason for low reporting rates and the minimal application of laws addressing offenses beyond obscenity and pornography is the general public's lack of understanding, especially among female victims.[151]

Legislation typically seeks to impose penalties such as imprisonment, fines, or compensation for victims. The focus of the law should extend beyond this.

[151] Cybercrime Against Women, https://pib.gov.in/PressReleseDetailm.aspx?PRID=1881404 accessed 10th march 2025

It needs to prioritize victim welfare and determine how to reintegrate individuals into society after experiencing the trauma of cyber-crimes. Police officers, cyber unit personnel, and trial judges can contribute more effectively by mandating the removal of online content shared or posted without the consent of the individual affected. Law enforcement officials should receive training in managing these cases, and there should be dedicated cyber unit officers in every police station. Additionally, there should be hotlines available for reporting such issues. Reputation management techniques and model behaviours should be provided to help victims alleviate their fears.

Raising awareness about legislative changes and developing a shared understanding of cyber-crime against women among various criminal justice stakeholders, including investigative officers, judges, and public prosecutors, is essential. It is equally important to acknowledge that existing laws are not equipped to handle all facets of cyber-crime against women in India. Women should be educated on preventative strategies, such as exercising caution when interacting with strangers online and safeguarding passwords and sensitive information that could jeopardize their privacy and security. As a measure to prevent incidents, women internet users in India should be informed about enhancing privacy settings on social networking platforms.[152]

Furthermore, there is an imperative need to implement stricter laws by amending the IT Act of 2000. Most cyber crimes should be classified as non-bailable offenses. Establishing dedicated units for investigations and developing an independent legal framework is necessary. A thorough data protection framework ought to be integrated into the legislation to enhance its effectiveness. Officers must receive specialized training to effectively address cyber crimes targeting women. The judiciary in India must play a crucial role in combating cybercrime against women in the country. The Indian government ought to pursue international collaboration with other nations for sharing information related to cybercrime. Therefore, the internet

[152] Ibid

can be seen as either a benefit or a drawback, depending on its usage. While it provides limitless opportunities and appeal, individuals should remain vigilant about their rights and privacy and be knowledgeable about utilizing applications and technologies in the most constructive way. [153]

[153] Ibid

Bibliography

Statutes and Bills

1. The Constitution of India, 1950
2. Indian Penal Code, 1860
3. Information Technology Act, 2000
4. Digital Personal Data Protection Act, 2023
5. Bharatiya Nyaya Sanhita (BNS), 2023
6. Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023
7. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
8. The Protection of Children from Sexual Offences (POCSO) Act, 2012
9. Juvenile Justice (Care and Protection of Children) Act, 2015
10. Press Council Act, 1978
11. United Nations Convention on the Rights of the Child, 1989
12. Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography, 2001
13. United Nations Convention against Transnational Organized Crime (UNCTOC), 2000
14. Sexual Offences Act, 2003 (UK)
15. Computer Misuse Act, 1990 (UK)
16. Theft Act, 1968 (UK)
17. Equality Act, 2010 (UK)
18. Crimes (Domestic and Personal Violence) Act, 2007 (Australia)
19. Cyber Crime Act, 2001 (Australia)

20. Criminal Code Act, 1995 & 1924 (Australia)

21. Crimes Act, 1900, 1958 (Australia)

22. Online Safety Bill, UK Parliament Bill 121, 2022–23

Books, Journals and Articles

1. Duggal, Pavan. Cyber Law – The Indian Perspective. Universal Law Publishing, 2021. ISBN: 9789391211404

2. Halder, Debarati and Jaishankar, K. Cyber Crime Against Women in India. Sage Publications, 2016. ISBN: 9789351507864

3. Nappinai, N.S. Technology Laws Decoded. LexisNexis, 2017. ISBN: 9788131252115

4. Roy, Rituparna. "Judiciary's Role in Combating Online Harassment of Women." Indian Bar Review, 2020. ISSN: 00194921; Volume: 47

5. Singh, Neha. "Judicial Interpretation of IT Act in India: A Gendered Lens." International Journal of Legal Research and Studies, 2021. ISSN: 2456-608X (Online) Volume: 6

6. Choudhury, Amit. "Revenge Porn and the Indian Judiciary." Indian Journal of Law and Legal Research, 2019. ISSN: 2582-8878; Volume-3.

7. Divan, Madhavi G. Facets of Media Law. Eastern Book Company, 2nd Edition, 2018. ISBN: 9789351455622

8. Sharma, Pratibha. "Digital Violence Against Women: Legal and Judicial Approaches." Indian Journal of Gender Studies, 2019. ISSN: 0971-5215; Volume-26.

9. Verma, Isha. "Judicial Trends in India on Online Abuse of Women." Indian Journal of Cyber Law, 2021. ISSN: 2347-5079; Volume: 8

10. Saxena, Ruchi. "Lack of Cyber Judicial Infrastructure in India." Journal of Cyber Law and Policy, 2020. ISSN: 2348-1234; Volume:5

11. Srivastava, Anjali. "Victim-Centric Justice in Cyber Law: A Comparative Study." Journal of Comparative Cyber Law, 2021. ISSN: 2349-8765; Volume: 7

12. Bansal, S. "Judicial Approaches to Cyber Violence Against Women in India: A Critical Analysis." Journal of Indian Law and Society, 2021. ISSN: 2277-5552; Volume 12

13. Chandra, Aparna et al. Seeking Justice in the Courts. Centre for Policy Research,

2018.

14. Bhatia, Gautam. Offend, Shock, or Disturb: Free Speech under the Indian Constitution. 2017.

15. Hoyle, Carolyn. Victim Support and the Judiciary. Oxford University Press, 2015. ISBN: 9780198723307

16. Brenner, Susan. Cybercrime: Criminal Threats from Cyberspace. Praeger, 2011. ISBN: 9780313365461, 9780313365478

17. Aneja, Anuradha. "Global Judicial Responses to Online Harassment." Journal of International Cyber Law and Policy, 2020. ISSN: 2457-1234, Volume 5.

18. Dr. Sanyogita & Anjali Singh. "Role of Judiciary in Curbing Cybercrimes against Women and Children in India." Commonwealth Law Review Journal, 2023. ISSN: 2581-3382; Volume 9.

19. Rathore, Rajveer Singh & Dr. Navneet Chahal. "Empowering Women against Cyber Crime: Legal Deficiencies and the Need for Reform in India." International Journal of Law Management & Humanities, 2024. ISSN: 2581-5369; Volume 7.

20. Arya, Nidhi. "Cyber Crime Scenario in India and Judicial Response." International Journal of Trend in Scientific Research and Development, 2019. ISSN: 2456-6470; Volume 3.

21. Singh, Priyal. "Patriarchal Face of Cyber Stalking." International Journal of Law Management And Humanities, 2019. International Journal of Law Management & Humanities; ISSN: 2581-5369 Volume: II, Issue II.

22. Verma, A. "The Rising Tide of Cyberstalking and Harassment in India: A Gendered Perspective." 2021. International Journal of Law Management & Humanities; ISSN: 2581 5369; Volume: IV, Issue I.

23. Nuruddin Khan and Dr. Shobha Gulati. "International Legislative Framework of Cybercrime." Journal of Political and Parliamentary Weekly (PPW)

9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 10 words)

Match Groups

199 Not Cited or Quoted **9%**
Matches with neither in-text citation nor quotation marks

0 Missing Quotations **0%**
Matches that are still very similar to source material

0 Missing Citation **0%**
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted **0%**
Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources

3% Publications

5% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.